世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 G11B 19/00	A1	(11) 国際公開番号 WO97/14147 (43) 国際公開日 1997年4月17日(17.04.97)

(21) 国際出願番号 PCT/JP96/02901

(22) 国際出願日 1996年10月4日(04.10.96)

(30) 優先権データ
特願平7/261266 1995年10月9日(09.10.95) JP

(71) 出願人（米国を除くすべての指定国について）
松下電器産業株式会社
(MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.)[JP/JP]
〒571 大阪府門真市大字門真1006番地 Osaka, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
植田 宏(UEDA, Hiroshi)[JP/JP]
〒573 大阪府枚方市御殿山南町4-3426 Osaka, (JP)
福島雄久(FUKUSHIMA, Yoshihisa)[JP/JP]
〒536 大阪府大阪市城東区関目六丁目14番C-508 Osaka, (JP)
伊藤基雅(ITO, Motomasa)[JP/JP]
〒536 大阪府大阪市城東区古市三丁目17番25-302号
Osaka, (JP)
舘林 誠(TATEBAYASHI, Makoto)[JP/JP]
〒665 兵庫県宝塚市売布一丁目16-21 Hyogo, (JP)

松尾なつめ(MATSUZAKI, Natsume)[JP/JP]
〒562 大阪府箕面市粟生間谷西一丁目6-7-803 Osaka, (JP)
(74) 代理人
弁理士 山本秀策(YAMAMOTO, Shusaku)
〒540 大阪府大阪市中央区馬見一丁目2番27号
クリスタルタワー15階 Osaka, (JP)

(81) 指定国 JP, US, 欧州特許 (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

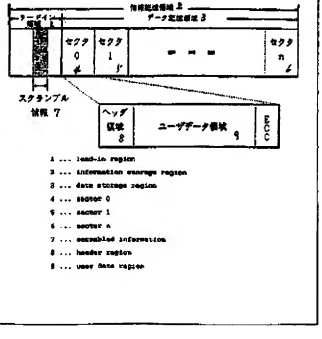
添付公開書類
国際調査報告書
請求の範囲の補正の期限前であり、補正書受領の際には再公開される。

(54)Title: **INFORMATION RECORDING MEDIUM, INFORMATION REPRODUCTION APPARATUS AND INFORMATION REPRODUCTION METHOD**

(54)発明の名称 情報記録媒体、情報再生装置および情報再生方法

(57) Abstract

An information recording medium including a lead-in region and a data recording region, wherein key information is recorded in the lead-in region and scrambled data are recorded in the data recording region. The scrambled data are descrambled on the basis of the key information.



(19)日本国特許庁（ＪＰ）　**再公表特許（Ａ１）**　(11)国際公開番号

ＷＯ９７／１４１４７

発行日　平成９年(1997)12月22日　(43)国際公開日　平成９年(1997)４月17日

(51)Int.Cl.[6]　識別記号　庁内整理番号　ＰＩ
Ｇ１１Ｂ　19/00

審査請求　未請求　予備審査請求　未請求（全 90 頁）

出願番号　特願平9－514906
(21)国際出願番号　ＰＣＴ／ＪＰ９６／０２９０１
(22)国際出願日　平成８年(1996)10月４日
(31)優先権主張番号　特願平7－261266
(32)優先日　平７(1995)10月９日
(33)優先権主張国　日本（ＪＰ）
(81)指定国　ＥＰ(ＡＴ, ＢＥ, ＣＨ, ＤＥ, ＤＫ, ＥＳ, ＦＩ, ＦＲ, ＧＢ, ＧＲ, ＩＥ, ＩＴ, ＬＵ, ＭＣ, ＮＬ, ＰＴ, ＳＥ), ＪＰ, ＵＳ

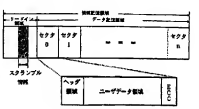
(71)出願人　松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　植田　宏
大阪府枚方市御殿山南町４－3426
(72)発明者　福島　健久
大阪府大阪市城東区関目６丁目14番Ｃ－506
(72)発明者　伊藤　基吉
大阪府大阪市城東区古市３丁目17番25－302号
(72)発明者　鎗林　誠
兵庫県宝塚市光市１丁目16－21
(74)代理人　弁理士　山本　秀策

最終頁に続く

(54)【発明の名称】　情報記録媒体、情報再生装置および情報再生方法

(57)【要約】
情報記録媒体は、リードイン領域とデータ記録領域とを有している。リードイン領域には、鍵情報が記録される。データ記録領域には、スクランブルされたデータが記録される。スクランブルされたデータは、鍵情報に基づいてデスクランブルされる。

図1



【特許請求の範囲】

１．リードイン領域とデータ記録領域とを有する情報記録媒体であって、

該リードイン領域には、鍵情報が記録され、

該データ記録領域には、スクランブルされたデータが記録され、

該スクランブルされたデータは、該鍵情報に基づいてデスクランブルされる、情報記録媒体。

２．リードイン領域とデータ記録領域とを有する情報記録媒体であって、

該リードイン領域には、第１の鍵情報が記録され、

該データ記録領域には、第２の鍵情報と、スクランブルされたデータとが記録され、

該スクランブルされたデータは、該第１の鍵情報に基づいて該第２の鍵情報を変換することによって得られる情報に基づいてデスクランブルされる、情報記録媒体。

３．前記データ記録領域は、複数のセクタに分割されており、該複数のセクタのそれぞれは、セクタを識別する情報を記録するセクタヘッダ領域と前記スクランブルされたデータを記録するメインデータ領域とを含んでおり、前記第２の鍵情報は、該セクタヘッダ領域に記録されている、請求項２に記載の情報記録媒体。

４．前記第２の鍵情報は、前記第１の鍵情報によって暗号化されており、前記鍵情報は、該暗号化された第２の鍵情報を復号化することによって得られる、請求項２に記載の情報記録媒体。

５．前記第１の鍵情報は、マスター鍵情報によって暗号化されている、請求項４に記載の情報記録媒体。

６．前記リードイン領域には、複数の第１の鍵情報が記録されており、該複数の第１の鍵情報は、複数の異なるマスター鍵情報によってそれぞれ暗号化されている、請求項４に記載の情報記録媒体。

７．前記情報記録媒体には、前記データ記録領域に記録されるデータがスクランブルされているか否かをポすスクランブルフラグがさらに記録されている、請求項２に記載の情報記録媒体。

8．前記データ記録領域は、複数のセクタに分割されており、該複数のセクタのそれぞれは、セクタを識別する情報を記録するセクタヘッダ領域と前記スクランブルされたデータを記録するメインデータ領域とを含んでおり、前記スクランブルフラグは、該セクタヘッダ領域に記録されている、請求項7に記載の情報記録媒体。

9．前記データ記録領域は、複数のファイルを記録する領域と、該複数のファイルを管理する情報を記録するファイル管理領域とを含んでおり、前記スクランブルフラグは、該ファイル管理領域に記録されている、請求項7に記載の情報記録媒体。

10．前記リードイン領域には、前記スクランブルされたデータを読み出す読み出し装置と該スクランブルされたデータをデスクランブルするデスクランブル回路を含むデコード装置との間で相互認証を行うための相互認証鍵情報がさらに記録されている、請求項2に記載の情報記録媒体。

11．前記情報は、乱数系列を生成するための初期値であり、前記スクランブルされたデータは、該乱数系列に対して論理演算を行うことによりデスクランブルされる、請求項2に記載の情報記録媒体。

12．前記データ記録領域は、複数のセクタに分割されており、該複数のセクタのそれぞれは、セクタを識別する情報を記録するセクタヘッダ領域と前記スクランブルされたデータを記録するメインデータ領域とを含んでおり、前記情報記録媒体の用途を識別する情報が該セクタヘッダ領域に記録されている、請求項2に記載の情報記録媒体。

13．情報記録媒体から、スクランブルされたデータと該スクランブルされたデータをデスクランブルするために使用される鍵情報とを読み出す読み出し回路と、

該スクランブルされたデータをデスクランブルするデスクランブル回路を含むデコード装置に該スクランブルされたデータを送信する前に、該鍵情報に対応する情報を該デコード装置に送信することを認証する認証回路と

を備えた情報再生装置。

14．前記情報記録媒体は、リードイン領域とデータ記録領域とを有しており、前記鍵情報は、該リードイン領域に記録される第1の鍵情報と、該データ記録領域に記録される第2の鍵情報とを含む、請求項13に記載の情報再生装置。

15．情報記録媒体からスクランブルされたデータと該スクランブルされたデータをデスクランブルするために使用される鍵情報とを読み出す読み出し装置から、該スクランブルされたデータを受信する前に、該鍵情報に対応する情報を該読み出し装置から受信することを認証する認証回路と、

該読み出し装置から受信した該スクランブルされたデータをデスクランブルするデスクランブル回路と

を備えた情報再生装置。

16．前記情報記録媒体は、リードイン領域とデータ記録領域とを有しており、前記鍵情報は、該リードイン領域に記録される第1の鍵情報と、該データ記録領域に記録される第2の鍵情報とを含む、請求項15に記載の情報再生装置。

17．前記デスクランブル回路は、該第1の鍵情報に基づいて該第2の鍵情報を変換することによって得られる情報に基づいて前記スクランブルされたデータをデスクランブルする、請求項16に記載の情報再生装置。

18．情報記録媒体から、スクランブルされたデータと該スクランブルされたデータをデスクランブルするために使用される鍵情報とを読み出す読み出し回路と、

該スクランブルされたデータをデスクランブルするデスクランブル回路を含むデコード部と、

該デコード部に該スクランブルされたデータを送信する前に、該鍵情報に対応する情報を該デコード部に送信することを認証する認証回路と

を備えた情報再生装置。

19．前記情報記録媒体は、リードイン領域とデータ記録領域とを有しており、前記鍵情報は、該リードイン領域に記録される第1の鍵情報と、該データ記録領域に記録される第2の鍵情報とを含む、請求項18に記載の情報再生装置。

20．前記デスクランブル回路は、該第1の鍵情報に基づいて該第2の鍵情報を

変換することによって得られる情報に基づいて前記スクランブルされたデータをデスクランブルする、請求項１９に記載の情報再生装置。

２１．前記情報記録媒体には、前記データ記録領域に記録されるデータがスクランブルされているか否かを示すスクランブルフラグがさらに記録されており、

前記情報再生装置は、

該スクランブルフラグに応じて、前記認証回路を起動するか否かを制御する制御回路をさらに備えている、請求項１８に記載の情報再生装置。

２２．前記認証回路による認証は、所定の関数を用いて行われる、請求項１８に記載の情報再生装置。

２３．前記認証回路による認証は、時間と共に変化する情報を用いて行われる、請求項１３、１５および１８のいずれかに記載の情報再生装置。

２４．前記認証回路は、認証処理が正常に終了した場合にバス鍵情報を生成し、該バス鍵情報を用いて前記第１の鍵情報と前記第２の鍵情報とを暗号化する、請求項１９に記載の情報再生装置。

２５．前記認証回路は、前記バス鍵情報を用いて前記暗号化された第１の鍵情報と前記暗号化された第２の鍵情報とを復号化する、請求項２４に記載の情報再生装置。

２６．情報記録媒体からスクランブルされたデータと該スクランブルされたデータをデスクランブルするために使用される鍵情報とを読み出す読み出し装置と、該スクランブルされたデータをデスクランブルするデスクランブル回路を含むデコーダ装置とを用いて、該スクランブルされたデータを再生する情報再生方法であって、

該読み出し装置と該デコード装置との間で相互認証処理を行うステップと、

該読み出し装置と該デコード装置との間で相互認証処理が正常に終了した場合に、該読み出し装置と該デコード装置とに共通するバス鍵情報を生成するステップと、

該バス鍵情報に応じて該鍵情報を暗号化するステップと、

該暗号化された鍵情報を該読み出し装置から該デコード装置に送信するステップと

を包含する情報再生方法。

【発明の詳細な説明】

情報記録媒体、情報再生装置および情報再生方法

技術分野

本発明は、プログラムデータ、音声情報、映像情報を含む情報信号を記録する情報記録媒体と、情報記録媒体に記録された情報を再生する情報再生装置および情報再生方法とに関する。

背景技術

従来、プログラムデータや音声情報、映像情報の情報記録媒体としては、フロッピーディスクやCD ROM (Compact Disk - Read Only Memory) などが知られている。特にCD-ROMは、600MB以上の大容量を有することや制作費用が安価になったこと等の理由で、各種ソフトウェアの頒布にさかんに用いられている。

一方、近年のパーソナルコンピュータの高速化によって、パーソナルコンピュータ上で映像および音声データ（以下、AVデータと称す）を出力する需要が急速に高まっている。例えばMPEG1 (Moving Picture Experts Group) と呼ばれる映像圧縮方式を用いてデータ圧縮を施したディジタルデータファイルを、CD-ROMなどに記録して頒布するようなアプリケーションが増加している。しかしながらMPEG1方式は一般に、大容量となる映像データを高い圧縮率を用いて圧縮するために、映像の劣化も著しい。従って、映画等の高品質な映像を要求される用途には不適当であった。

そこで近年、5GB近い大容量を有する光ディスクにMPEG2方式と呼ばれる、より高度な映像圧縮方式を用いて、高品質な映像データを記録する開発が行われている。DVD (Digital Video Disk) と呼ばれるその光ディスクは、大容量性を生かして、2時間以上もの高品質なディジタルAVデータを記録することが可能であり、次世代のAVデータ記録媒体として大いに期待されている。またその一方でDVDは、パーソナルコンピュータと接続されてDVDを再生するDVDドライブによって、高品質なAVデータをパーソナルコンピュータ上で再生することが可能となるとともに、計算機ソフトウェアの頒布媒体としてもCD

ROMに替わる情報記録媒体として期待されている。

しかしながら、パーソナルコンピュータの周辺装置としてのDVDドライブが市場に出回れば、DVDに記録されたディジタルデータがパーソナルコンピュータに出力され、容易にハードディスクやMO (Magneto Optical Disk) 等の書き換え型メディアにコピーすることが可能となる。前記のようなディジタルAVデータのコピーが容易に行えれば、DVDに記録されたAVデータがその著作者の許可なく違法にコピーされたり、改竄を施されて頒布されるなどの問題が生じ、著作者の権利を保護することが極めて困難となる。このことは、データの著作者にとって不利益をもたらすばかりでなく、著作者がコピーされることを考慮して価格設定を行うことやデータの改竄をおそれてディスクの製造を行わない等の措置がとられた場合においては、ユーザへの不利益も生ずる可能性がある。前記の課題を以下では、第1の課題と称する。

一方、AVデータの記録された情報記録媒体の用途としては、様々な用途が考えられる。これらの用途の中には、情報記録媒体があらゆる再生装置で再生可能となることが逆に問題となる用途も存在し、その様な用途では再生可能な再生装置と再生不可能な再生装置とに分別できることが好ましい。例えば、一般にカラオケディスクと呼ばれるような、再生される音楽に合わせてその歌詞を含んだ映像データが記録されるようなディスクには、一般家庭で個人的に使用されるディスク（以下、民生用ディスクと称す）と、利用者が一定の料金を支払ってカラオケを楽しむような施設において使用されるディスク（以下、業務用ディスクと称す）とが存在する。業務用ディスクが限られた使用者に大量に納入することを前提に製造されるために、低価格で供給されるのに対し、民生用ディスクは単品販売のために比較的高価格で販売されている。

しかしながら、業務用ディスクと民生用ディスクとが全く同一フォーマットであった場合には、業務用ディスクが民生用として一般市場で安価に販売される可能性がある。従って、市場における民生用ディスクの適正な価格での流通を妨げ、ディスク製造者および正規に民生用ディスクを購入するユーザの不利益となる。従ってこの様な用途では、民生用ディスクと業務用ディスクで再生可能な再生

装置が分離できることが望ましい。また別の例としては、倫理的な問題のある内容を記録したディスクを再生する場合がある。倫理的な問題があるか否かを判定する基準は各国ごとに異なる。従ってある国では再生されるべきディスクが、他の国で再生されるのが望ましくない場合が生ずる。従って、倫理上問題があるディスクはその販売が許可される特定の国でのみ再生されるような仕組みが必要である。以上の様に、ディスクの用途に応じて再生可能な再生装置と再生不可能な再生装置とを分別できないという課題があった。この課題を、以下では第2の課題と称する。

上記の2つ課題を解決するための一つの手段として、情報記録ディスクに記録するデータをスクランブル（又は暗号化）して記録する方法がある。すなわち、前記第1の課題に対しては、パーソナルコンピュータにおけるコピー動作時に、ある鍵をもとにスクランブルの施されたデータを返送し、デスクランブルするための鍵を返送しないことによりコピー動作を防止できる（コピー動作は行われるが、そのデスクランブルが行えないために、コピー動作の意味をなさない）。

また、前記第2の課題に対しては、ディスクの内容に応じて異なるスクランブルを施したディスクを作成することで、デスクランブル可能な装置とデスクランブル不可能な装置とを分類できる。このように、記録データのスクランブル（又は暗号化）は前記の2つの問題に有効であるが、データをデスクランブルするための方法又は鍵をどのように指定するかが問題となる。

データ領域に暗号化を施す第1の従来例として、特開平7－249264号公報の図3のCD－ROMでは、暗号化されたデータセクタとは異なるセクタのメインデータ領域に暗号鍵を記録する方式が提案されている。本従来例では、記録時に暗号化されたデータとその暗号鍵をCD－ROMに記録し、再生時にはパーソナルコンピュータから再生装置に対して暗号鍵の読み出し命令を行った後に暗号化データを復号することにより、データ再生を実現するというものである。本方法は、暗号鍵の変更が容易に行えるという利点がある。

また、第2の従来例として、特開平7－85574号公報の図3に示されるように再生装置の光ヘッドが走査しないディスクの領域に暗号化キーを記録する方

式が提案されている。本従来例では、一般のパーソナルコンピュータから暗号鍵を読み出されることを防止するために、コピー動作において暗号鍵はコピーされず、違法なコピー動作が意味をなさない。

しかしながら、前記第1の従来法の暗号鍵はセクタのメインデータ領域に記録されているため、係るディスクの記録時に用いられた暗号鍵を一般のパーソナルコンピュータから容易に読み出すことができる。従って、暗号鍵と暗号化データをユーザが読み出すことができるために、暗号の解読を行われる危険性が高い。

また第2の従来法では、暗号鍵を再生装置の光ヘッドが走査しない領域に記録するために、暗号鍵を読み出すためにはデータ記録領域からデータを読み出す読み出し手段に加えて暗号鍵読み出し専用の読み出し手段が必要になるという問題が生ずる。

本発明は、情報記録媒体に記録された内容が違法にコピーされることを確実に防止する強固な著作権保護を実現するためのデータ構造を有する情報記録媒体と、特別なデータ読み出し手段を設けることなく前記情報記録媒体からのデータ再生が可能であり、かつ、前記課題1および2を解決するための情報再生装置および情報再生方法を提供することを目的とする。

発明の開示

本発明の情報記録媒体は、リードイン領域とデータ記録領域とを有する情報記録媒体であって、該リードイン領域には、鍵情報が記録され、該データ記録領域には、スクランブルされたデータが記録され、該スクランブルされたデータは、該鍵情報に基づいてデスクランブルされる。

本発明の他の情報記録媒体は、リードイン領域とデータ記録領域とを有する情報記録媒体であって、該リードイン領域には、第1の鍵情報が記録され、該データ記録領域には、第2の鍵情報と、スクランブルされたデータとが記録され、該スクランブルされたデータは、該第1の鍵情報に基づいて該第2の鍵情報を変換することによって得られる情報に基づいてデスクランブルされる。

ある実施形態では、前記データ記録領域は、複数のセクタに分割されており、該複数のセクタのそれぞれは、セクタを識別する情報を記録するセクタヘッダ領

域と前記スクランブルされたデータを記録するメインデータ領域とを含んでおり、前記第２の鍵情報は、該セクタヘッダ領域に記録されている。

他の実施形態では、前記第２の鍵情報は、前記第１の鍵情報によって暗号化されており、前記情報は、該暗号化された第２の鍵情報を復号化することによって得られる。

他の実施形態では、前記第１の鍵情報は、マスター鍵情報によって暗号化されている。

他の実施形態では、前記リードイン領域には、複数の第１の鍵情報が記録されており、該複数の第１の鍵情報は、複数の異なるマスター鍵情報によってそれぞれ暗号化されている。

他の実施形態では、前記情報記録媒体には、前記データ記録領域に記録されるデータがスクランブルされているか否かを示すスクランブルフラグがさらに記録されている。

他の実施形態では、前記データ記録領域は、複数のセクタに分割されており、

該複数のセクタのそれぞれは、セクタを識別する情報を記録するセクタヘッダ領域と前記スクランブルされたデータを記録するメインデータ領域とを含んでおり、前記スクランブルフラグは、該セクタヘッダ領域に記録されている。

他の実施形態では、前記データ記録領域は、複数のファイルを記録する領域と、該複数のファイルを管理する情報を記録するファイル管理領域とを含んでおり、前記スクランブルフラグは、該ファイル管理領域に記録されている。

他の実施形態では、前記リードイン領域には、前記スクランブルされたデータを読み出す読み出し装置と該スクランブルされたデータをデスクランブルするデスクランブル回路を含むデコード装置との間で相互認証を行うための相互認証鍵情報がさらに記録されている。

他の実施形態では、前記情報は、乱数系列を生成するための初期値であり、前記スクランブルされたデータは、該乱数系列に対して論理演算を行うことによりデスクランブルされる。

他の実施形態では、前記データ記録領域は、複数のセクタに分割されており、

該複数のセクタのそれぞれは、セクタを識別する情報を記録するセクタヘッダ領域と前記スクランブルされたデータを記録するメインデータ領域とを含んでおり、前記情報記録媒体の用途を識別する情報が該セクタヘッダ領域に記録されている。

本発明の情報再生装置は、情報記録媒体から、スクランブルされたデータと該スクランブルされたデータをデスクランブルするために使用される鍵情報とを読み出す読み出し回路と、該スクランブルされたデータをデスクランブルするデスクランブル回路を含むデコード装置に該スクランブルされたデータを送信する前に、該鍵情報に対応する情報を該デコード装置に送信することを認証する認証回路とを備えている。

ある実施形態では、前記情報記録媒体は、リードイン領域とデータ記録領域とを有しており、前記鍵情報は、該リードイン領域に記録される第１の鍵情報と、該データ記録領域に記録される第２の鍵情報とを含む。

本発明の他の情報再生装置は、情報記録媒体からスクランブルされたデータと該スクランブルされたデータをデスクランブルするために使用される鍵情報とを読み出す読み出し装置から、該スクランブルされたデータを受信する前に、該鍵情報に対応する情報を該読み出し装置から受信することを認証する認証回路と、該読み出し装置から受信した該スクランブルされたデータをデスクランブルするデスクランブル回路とを備えている。

ある実施形態では、前記情報記録媒体は、リードイン領域とデータ記録領域とを有しており、前記鍵情報は、該リードイン領域に記録される第１の鍵情報と、該データ記録領域に記録される第２の鍵情報とを含む。

他の実施形態では、前記デスクランブル回路は、該第１の鍵情報に基づいて該第２の鍵情報を変換することによって得られる情報に基づいて前記スクランブルされたデータをデスクランブルする。

本発明の他の情報再生装置は、情報記録媒体から、スクランブルされたデータと該スクランブルされたデータをデスクランブルするために使用される鍵情報とを読み出す読み出し回路と、該スクランブルされたデータをデスクランブルする

デスクランブル回路を含むデコード部と、該デコード部に該スクランブルされたデータを送信する前に、該鍵情報に対応する情報を該デコード部に送信することを認証する認証回路とを備えている。

ある実施形態では、前記情報記録媒体は、リードイン領域とデータ記録領域とを有しており、前記鍵情報は、該リードイン領域に記録される第１の鍵情報と、該データ記録領域に記録される第２の鍵情報とを含む。

他の実施形態では、前記デスクランブル回路は、該第１の鍵情報に基づいて該第２の鍵情報を変換することによって得られる情報に基づいて前記スクランブルされたデータをデスクランブルする。

他の実施形態では、前記情報記録媒体には、前記データ記録領域に記録されるデータがスクランブルされているか否かを示すスクランブルフラグがさらに記録されており、前記情報再生装置は、該スクランブルフラグに応じて、前記認証回路を起動するか否かを制御する制御回路をさらに備えている。

他の実施形態では、前記認証回路による認証は、所定の関数を用いて行われる。

他の実施形態では、前記認証回路による認証は、時間と共に変化する情報を用いて行われる。

他の実施形態では、前記認証回路は、認証処理が正常に終了した場合にバス鍵情報を生成し、該バス鍵情報を用いて前記第１の鍵情報と前記第２の鍵情報とを暗号化する。

他の実施形態では、前記認証回路は、前記バス鍵情報を用いて前記暗号化された第１の鍵情報と前記暗号化された第２の鍵情報とを復号化する。

本発明の情報再生方法は、情報記録媒体からスクランブルされたデータと該スクランブルされたデータをデスクランブルするために使用される鍵情報とを読み出す読み出し装置と、該スクランブルされたデータをデスクランブルするデスクランブル回路を含むデコーダ装置とを用いて、該スクランブルされたデータを再生する情報再生方法であって、該読み出し装置と該デコード装置との間で相互認証処理を行うステップと、該読み出し装置と該デコード装置との間で相互認証処理が正常に終了した場合に、該読み出し装置と該デコード装置とに共通するバス鍵情報を生成するステップと、該バス鍵情報に応じて該鍵情報を暗号化するステップと、該暗号化された鍵情報を該読み出し装置から該デコード装置に送信するステップとを包含する。

図面の簡単な説明

図１は、本発明に係る情報記録媒体のデータ構造を示す図である。

図２（ａ）および（ｂ）は、図１に示す情報記録媒体のリードイン領域に記録されるスクランブル情報の構造を示す図である。

図３は、本発明に係る情報記録媒体の他のデータ構造を示す図である。

図４は、本発明に係る情報再生装置の構成を示すブロック図である。

図５は、本発明に係る情報再生装置の他の構成を示すブロック図である。

図６は、本発明に係る情報再生装置の他の構成を示すブロック図である。

図７は、本発明に係る情報再生装置の他の構成を示すブロック図である。

図８は、本発明に係る情報再生装置の他の構成を示すブロック図である。

図９（ａ）～（ｃ）はスクランブル処理方法の一例を説明するための図である。

図１０（ａ）～（ｆ）は、本発明に係る情報記録媒体のデータ構造を示す図である。

図１１（ａ）～（ｃ）は、ボリューム・ファイル管理領域中のディレクトリレコードのデータ構造を示す図である。

図１１（ｄ）は、スクランブル情報セクタのデータ構造を示す図である。

図１１（ｅ）は、スクランブルセクタのデータ構造を示す図である。

図１１（ｆ）は、非スクランブルセクタのデータ構造を示す図である。

図１２（ａ）～（ｃ）は、スクランブル方式の一例を説明するための図である。

図１３（ａ）～（ｃ）は、ボリューム・ファイル管理領域中のディレクトリレコードのデータ構造を示す図である。

図１３（ｄ）は、スクランブル情報セクタのデータ構造を示す図である。

図１３（ｅ）は、スクランブルセクタのデータ構造を示す図である。

図１３（ｆ）は、非スクランブルセクタのデータ構造を示す図である。

図１４は、本発明に係る情報再生装置５００の構成を示すブロック図である。

図１５は、情報再生装置５００に含まれる光ディスクドライブ５０９の構成を示すブロック図である。

図１６は、情報再生装置５００に含まれるＡＶデコードカード５０７の構成を示すブロック図である。

図１７は、本発明に係る情報再生装置８００の構成を示すブロック図である。

図１８は、情報再生装置８００に含まれるＳＣＳＩ制御回路内蔵ＡＶデコードカード８０１の構成を示すブロック図である。

図１９は、本発明に係る情報再生装置（光ディスクプレーヤ）１０００の構成

を示すブロック図である。

図２０は、デスクランブル回路１１０６の構成を示すブロック図である。

図２１は、デスクランブル回路１１０６によって実行されるデスクランブル処理の手順を示すフローチャートである。

図２２は、デスクランブル回路１３０８の構成を示すブロック図である。

図２３は、デスクランブル回路１３０８によって実行されるデスクランブル処理の手順を示すフローチャートである。

図２４は、デコーダ認証回路６０１の構成を示すブロック図である。

図２５は、ドライブ認証回路７０１の構成を示すブロック図である。

図２６は、光ディスクドライブ５０９とＡＶデコーダカード５０７又はＳＣＳＩ制御回路内蔵ＡＶデコーダカード８０１間の相互認証処理を説明するためのフローチャートである。

発明を実施するための最良の形態

以下、図面を参照しながら、本発明の実施の形態を説明する。

（第１の実施形態）

図１は、本発明に係る情報記録媒体のデータ構造を示す。以下、情報記録媒体としてディスクを例にとり説明する。しかし、本発明に係る情報記録媒体は、ディスクに限定されず、任意の情報記録媒体であり得る。

一般に、ディスク上で何らかの情報が記録されている情報記録領域は、主として制御情報が記録されるリードイン領域と、ユーザデータが記録されるデータ記録領域とに大別される。また、データ記録領域はセクタと呼ばれる単位で区切られているのが一般的である。ここで、ディスク再生装置は、リードイン領域を直接的にアクセスすることができるが、ディスク再生装置以外の装置（例えば、パーソナルコンピュータ）は、リードイン領域を直接的にアクセスすることができない。

各セクタは、セクタを識別するためのセクタＩＤ（IDentifier）等が記録されるヘッダ領域と、ユーザデータが記録されるユーザデータ領域と、再生時の読み出し誤りを訂正するための符号が記録されるＥＣＣ（Error Correction Code）領域とを含む。本実施の形態では、セクタ中のユーザデータ領域に記録されるユーザデータに対してスクランブル処理が施されているものとする。従って、情報再生装置が同１のディスクからユーザデータを正しく再生するためには、そのユーザデータに対して施されているスクランブル処理方法を知る必要がある。

図１のディスクのリードイン領域の所定の位置には、ユーザデータに対して施されているスクランブル処理方法を定める情報（以下、本明細書において「スクランブル情報」という）が記録されている。情報再生装置は、スクランブル情報が記録された領域を読み出し、そのスクランブル情報を解釈し、そのスクランブル情報に従った逆スクランブル処理をユーザデータに対して施す。これにより、ユーザデータを正しく再生することが可能となる。

ここで、一般に知られているスクランブル処理方法の一例を図９を用いて説明する。

図９（ａ）は、１つのセクタが、セクタＩＤ領域と、２０４８バイトのユーザデータ領域と、ＥＣＣ領域とから成ることを示している。ユーザデータ領域には、データバイト列D_0，D_1，・・・，D_{2047}が記録される。データバイト列D_0，D_1，・・・，D_{2047}は、記録されるべき（スクランブル処理前の）データバイト列D'_0，D'_1，・・・，D'_{2047}と乱数系列S_0，S_1，・・・，S_{2047}と

の論理演算によって求められる。例えば、その論理演算は、排他的論理和であり得る。ここで、乱数系列S_0，S_1，・・・，S_{2047} は、与えられた初期値に対して一意に定まるものとする。

乱数系列S_0，S_1，・・・，S_{2047} の初期値を求めるために、セクタ中の所定ビット列（例えば、セクタＩＤ領域の所定位置の３ビット）に基づいて図９（ｂ）に示すようなテーブルが参照される。例えば、セクタＩＤ領域の所定位置の３ビットが（０，０，１）である場合には、そのテーブルより初期値が１００Ｆｈと求まり、乱数系列B_0，B_1，・・・，B_{2047} （S_0，S_1，・・・，S_{2047} に相当する）が一意に定まる。

与えられた初期値から乱数系列S_0，S_1，・・・，S_{2047} を発生する方法としては、例えば、図９（ｃ）に示すようなシフトレジスタを用いる方法が知られている。

スクランブル処理方法としては、この他にも、ユーザデータのバイト列内で所定ビットを入れ替える等の他の方法を用いることも可能である。以下では、図９で述べたスクランブル処理方法を用いて、説明を行う。

図２は、図１に示されるディスクのリードイン領域の所定位置に記録されるスクランブル情報の構造を示す。

図２（ａ）に示されるように、この例では、スクランブル情報は、スクランブル処理に用いる乱数系列の初期値を得るテーブルを指定する識別子である。なお、そのテーブル以外のスクランブル処理方法を特定するための情報はあらかじめ定義されているものとする。

例えば、スクランブル情報の内容が（１，０）であることは、あらかじめ定義された図２（ｂ）に示される４つのテーブルのうち、テーブル２がスクランブル処理に用いられたことを示す。情報再生装置は、図２（ｂ）の４つのテーブルを格納するメモリを有しており、スクランブル情報に応じて逆スクランブル処理に使用するテーブルを切り替える。これにより、ユーザデータに対する逆スクランブル処理を正しく実行することが可能となる。

図３は、本発明に係るディスクの他のデータ構造を示す。図３に示されるディスクのリードイン領域には、初期値テーブルが直接記録されいる。そのディスクのデータ記録領域には、その初期値テーブルを用いて発生された乱数系列によってスクランブル処理が施されたユーザデータが記録されている。ここで、図３に示したスクランブル処理方法が有する他のパラメータはあらかじめ一意に定められているものとする。

情報再生装置は、ディスクのリードイン領域に記録された初期値テーブルを読み出し、その初期値テーブルを解釈する。その後、情報再生装置は、初期値テーブルに従った逆スクランブル処理手順を設定し、その逆スクランブル処理手順に従ってユーザデータを逆スクランブルする。これによって、スクランブルされたユーザデータを正しく再生することができる。

また、ディスクをある特定の逆スクランブル処理手順しか有さない情報再生装置で再生することは、そのディスクの初期値テーブルと情報再生装置の初期値テーブルが一致する場合に限られ、それ以外の場合は正しく再生することは不可能となる。

なお、上述した実施の形態では、図９で示したスクランブル処理方法における乱数系列の初期値テーブルを変更する方法を示した。しかし、図９で示したスクランブル処理方法である必要はなく、全く異なるスクランブル処理方法を使用することも可能である。また、図９で示したスクランブル処理方法において、初期値テーブルの他にも変更可能なパラメータは多様にあり（例えば初期値テーブルを参照するためのビット列の取り方や乱数を発生させるシフトレジスタの構成など）、変更可能なパラメータの各々や組み合わせに識別子を与えることも可能となる。

上述したように、本発明に係る情報記録媒体によれば、用途や複製許可／不許可に応じてスクランブル処理方法を変更することが可能となる。その結果、不正な再生（例えば業務用ディスクを民生用ディスク再生装置で再生すること）や不正なコピーを防止することができる。

（第２の実施形態）

図４は、本発明に係る情報再生装置の構成を示す。情報再生装置は、ホストコ

ンピュータ１と、ディスク３に記録されたデータを再生するディスク再生装置２とを含んでいる。

ホストコンピュータ１は、インタフェース部（Ｉ／Ｆ部）４と、映像情報を表示可能な形式に復号するＡＶデコーダ６と、表示装置７に映像情報を送出するビデオボード８と、ＣＰＵ１０と、ＤＲＡＭ（Dynamic Random Access Memory）などの内部メモリ１１とを含んでいる。ビデオボード８と、ＣＰＵ１０と、内部メモリ１１とは、バス９を介して相互に接続される。ビデオボード８の出力は、表示装置（出力装置）７に接続されている。ハードディスクドライブ１２は、インタフェース部４に接続されている。

ディスク再生装置２は、インタフェース部５と、ディスク３からデータを読み出すための機構・信号処理回路・制御回路等を含むデータ再生部１３と、ディスク再生装置２を制御するマイクロプロセッサ１４とを含んでいる。

ホストコンピュータ１とディスク再生装置２とは、インタフェース部４、５を介して接続されている。例えば、インタフェース部４、５は、ＳＣＳＩ（Small Computer System Interface）やＡＴＡＰＩ（AT Attachment Packet Interface）等の既存のインタフェース又は独自に定義されたインタフェースによって接続され得る。

ディスク再生装置２は、ディスク再生装置２のリセット時やディスク３の交換時において、ディスク３のリードイン領域に記録されたスクランブル情報を読み出し、そのスクランブル情報を解釈し、そのスクランブル情報に従った逆スクランブル処理手順をデータ再生部１３に設定する。

ホストコンピュータ１は、ディスク３のデータ記録領域に記録されたユーザデータを出力装置７に表示するために、ディスク再生装置２に対してインタフェース部４、５を介して再生専用コマンド（以下、ＰｌａｙＡＶコマンドと称する）を発行する。ディスク再生装置２は、ＰｌａｙＡＶコマンドに応答して、スクランブル情報に従って逆スクランブル処理が施されたユーザデータをホストコンピュータ１に送信する。

ホストコンピュータ１のインタフェース部４は、ＰｌａｙＡＶコマンドを使用

してディスク再生装置２から受け取ったユーザデータはデータバス９には送らず、ＡＶデコーダ６にのみ送る。従って、ＰｌａｙＡＶコマンドを用いて得られたユーザデータをホストコンピュータ１に接続されたハードディスクドライブ１２等の書き換え可能媒体に記録することは不可能である。

ホストコンピュータ１は、ディスク３のデータ記録領域に記録されたユーザデータをハードディスク１２や内部メモリ１１に記録する必要がある場合には、データ読出しコマンド（以下、Ｒｅａｄコマンドと称する）を発行する。ディスク再生装置２は、そのＲｅａｄコマンドに応答して、ディスク３のコピーが許可されているか否かをあらかじめ保持しているスクランブル情報をもとに判定する。

ディスク再生装置２は、スクランブル情報で指定されるスクランブル方式がコピー許可されたタイプであるか否かによって、異なる動作をする。

ディスク再生装置２がディスク３のコピーが許可されていると判定した場合には、ディスク再生装置２の立ち上げ動作時にディスク３のリードイン領域から読み込んだスクランブル情報に従って逆スクランブル処理を施した正しいユーザデータをホストコンピュータ１に送信する。一方、ディスク再生装置２がディスク３のコピーが禁止されていると判定した場合には、スクランブル情報とは異なる逆スクランブル処理を施した誤ったユーザデータをホストコンピュータ１に送信する。あるいは、エラー処理を行う等を行うことによって、ディスク再生装置２が正しいデータをホストコンピュータ１に返送しないようにしてもよい。このようにして、不法な複製を防止することが可能となる。

ディスク３のコピーが許可されているか否かを示す情報（コピー許可情報）を得る方法としては、様々な方法がある。例えば、コピー許可情報がディスク３の所定の領域に記録されている場合には、ディスク再生装置２がディスク３のその所定の領域からコピー許可情報を読み出せばよい。あるいは、コピー許可情報に応じてスクランブル処理方式が限定されている場合には、読み出されたスクランブル情報によってコピー許可情報を特定することができる。

あるいは、コピー許可情報は、スクランブル情報の一部によって表され得る。例えば、スクランブル情報が複数のビットからなる場合において、その複数のビ

ットのうち1ビットでコピー許可情報を表すことにしてもよい。このように、スクランブル情報は、コピーが許可されたデータに施すスクランブル方式と、コピーが禁止されたデータに施すスクランブル方式とを明確に区別するために使用され得る。従って、ディスク3からスクランブル情報を読み出すことにより、コピーが許可されているか否かを判定することが可能となる。以下、コピー許可情報はスクランブル情報の一部によって表されるとして説明する。

図5は、本発明に係る情報再生装置の他の構成を示す。図5の情報再生装置では、図4のホストコンピュータ1において独立していたAVデコーダ6とインタフェース部4とが、一体化した構成となっている。その他の構成は、図4の情報再生装置の構成と同様である。

PlayAVコマンドがホストコンピュータ1から発行されると、スクランブル情報に従って逆スクランブル処理を施されたユーザデータがディスク再生装置2からホストコンピュータ1に送信される。そのユーザデータは、AVデコーダ6によってAVデコードされて、その後、ビデオボード8に直接入力される。他の動作については、図4を用いて説明した実施の形態の情報再生装置と同様であるため、説明を省略する。

図6は、本発明に係る情報再生装置の他の構成を示す。図6の情報再生装置は、AVデコーダ6と一体化したインタフェース部4bと、インタフェース部4bとは独立したインタフェース部4aとを含んでいる。その他の構成は、図5の情報再生装置と同様である。

AVデコーダ6内のインタフェース部4bからはPlayAVコマンドのみが発行される。一方、Readコマンドは、インタフェース部4bとは独立したインタフェース部4aから発行される。他の動作については、図4を用いて説明した実施の形態の情報再生装置と同様であるため、説明を省略する。

図7は、本発明に係る情報再生装置の他の構成を示す。図7の情報再生装置では、データを表示可能な形式に変換するAVデコーダ6がディスク再生装置2に内蔵されている。従って、ディスク再生装置2をホストコンピュータ1に接続することは不要である。

以下に本構成の情報再生装置の動作を説明する。図7のディスク再生装置2において、マイクロプロセッサ14は、図1に示すディスクからスクランブル情報を読み出し、そのスクランブル情報を解釈し、そのスクランブル情報に従った逆スクランブル処理をユーザデータに施す。逆スクランブル処理が施されたユーザデータはAVデコーダに送られる。ユーザデータは、AVデコーダ6によってAVデコードされ、出力装置7に出力される。このようにしてディスク3に記録されたユーザデータの再生が可能となる。

しかしながら、ディスク再生装置2で再生することが好ましくないスクランブル情報がディスク3に記録されていた場合には、ディスク再生装置2は正しい再生を行わないことも可能である。例えば、ディスク3がカラオケ用途に使用される業務用ディスクであると仮定する。この場合において、そのディスク3が民生用ディスク再生装置に装着された場合には、民生用ディスク再生装置がディスク3に記録されたデータの再生を行わないようにすることも可能である。民生用ディスク再生装置は、ディスク3に記録されたスクランブル情報から民生用ディスクには使用されないスクランブル処理方法であるか否かを判定することができるからである。このように、ディスク3の用途に応じて使用可能なスクランブル処理方法を限定することにより、ディスク再生装置2がスクランブル情報に基づいて、ディスク3に記録されたデータを再生すべきか否かを判定することが可能となる。

また、特定の逆スクランブル処理のみを行うことが可能なディスク再生装置に対して、その逆スクランブル処理に対応しないスクランブル処理方法でスクランブルされたデータを記録したディスクを製造することにより、そのディスク再生装置がそのディスクに記録されたデータを再生することを禁止することが可能となる。

図8は、本発明に係る情報再生装置の構成を示す。情報再生装置は、ホストコンピュータ1と、ディスク再生装置11とを含んでいる。ホストコンピュータ1は、図8には示されていない。ホストコンピュータ1の構成は、図4～図6のホストコンピュータ1の構成と同様である。

ディスク再生装置１１は、インタフェース部（Ｉ／Ｆ部）５と、ディスク３に記録されたデータを読み出すデータ再生部１３と、ディスク再生装置１１を制御するマイクロプロセッサ１４と、逆スクランブル回路部１５と、復調・エラー訂正部１６と、マイクロプロセッサ１４によって実行されるプログラム等を格納するＲＯＭ（Read Only Memory）１７と、データ処理用ＲＡＭ（Random Access Memory）２０とを含んでいる。インタフェース部５と、データ再生部１３と、マイクロプロセッサ１４と、逆スクランブル回路部１５と、復調・エラー訂正部１６と、データ処理用ＲＡＭ２０とは、内部データバス１９を介して相互に接続されている。逆スクランブル回路部１５は、初期値テーブル格納用メモリ１８を含んでいる。

マイクロプロセッサ１４は、電源投入時やディスク３が交換された時等に、ディスク３からスクランブル情報を読み出し、そのスクランブル情報を解釈する。

ディスク３が図２に示すデータ構造を有する場合には、マイクロプロセッサ１４は、ＲＯＭ１７に予め格納された複数の初期値テーブルの中から、スクランブル情報の内容に従って１つの初期値テーブルを選択する。マイクロプロセッサ１４は、選択された初期値テーブルを逆スクランブル回路部１５内の初期値テーブル格納用メモリ１８に格納する。初期値テーブル格納用メモリ１８は、例えば、ＲＡＭであり得る。あるいは、初期値テーブル格納用メモリ１８がＲＯＭである場合には、そのＲＯＭに複数の初期値テーブルを予め格納しておいてもよい。

ホストコンピュータ１がＰｌａｙＡＶコマンドを発行すると、そのＰｌａｙＡＶコマンドは、ディスク再生装置２のインタフェース部５を介してマイクロプロセッサ１４に入力される。マイクロプロセッサ１４は、ＰｌａｙＡＶコマンドに応答して、スクランブルされたユーザデータに対して逆スクランブル処理を行うように逆スクランブル回路部１５に指示する。逆スクランブル回路部１５は、初期値テーブル格納用メモリ１８に格納された初期値テーブルに従って逆スクランブル処理を行う。逆スクランブル処理が施されたデータは、インタフェース部５を介してホストコンピュータ１に送信される。このようにして、ディスク３に記録されたデータを再生することが可能となる。

一方、ホストコンピュータ１がＲｅａｄコマンドを発行すると、そのＲｅａｄコマンドは、ディスク再生装置１１のインタフェース部５を介してマイクロプロセッサ１４に入力される。このとき、マイクロプロセッサ１４は、ディスク３からあらかじめ読み出したスクランブル情報からコピーが許可されているスクランブル方式か否かを判定する。マイクロプロセッサ１４は、コピーが禁止されていると判定した場合には、スクランブル情報に対応する初期値テーブルとは異なる初期値テーブルを逆スクランブル回路部１５に設定する。あるいは、マイクロプロセッサ１４は、初期値テーブルを逆スクランブル回路部１５に設定することなく、ホストコンピュータ１にエラーを返送するようにしてもよい。このようにして、ディスク３に記録されたデータが再生されることを防止することができる。

また、マイクロプロセッサ１４がスクランブル情報からコピーが許可されていると判定した場合において、ディスク３が図３に示すデータ構造を有する場合には、マイクロプロセッサ１４は、ディスク３のリードイン領域から初期値テーブルを読み出し、その初期値テーブルを逆スクランブル回路部１５内の初期値テーブル格納用メモリ１８に格納する。初期値テーブル格納用メモリ１８は、書き込み可能なメモリ（例えば、ＲＡＭ）である。その他の処理は、ディスク３が図２に示すデータ構造を有する場合と全く同様であるので、ここでは省略する。

上述したように、本発明に係る情報再生装置によれば、情報記録媒体に記録されたスクランブル情報に応じて逆スクランブル処理方法を変更することが可能となる。これにより、複数種類の異なるスクランブル処理方法でスクランブルされたデータを正しく再生することが可能となる。

また、本発明に係る情報再生装置によれば、情報記録媒体に記録されたスクランブル情報に応じて情報再生装置が情報記録媒体に記録されたデータを再生すべきか否かを判定することができる。その結果、不法な複製を防止し、情報記録媒体に記録されたデータの著作権を保護することができる。

（第３の実施形態）

図１０（ａ）は、本発明に係る情報記録媒体のデータ構造を示す。情報記録媒体上の何らかのデータが記録されている情報記録領域は、リードイン領域と、デ

ータ記録領域と、リードアウト領域とを含む。リードイン領域には、情報再生装置が情報記録媒体を再生するために必要とする情報が記録されている。データ記録領域には、主としてユーザにとって有用なプログラムデータやＡＶデータ等のデータが記録されている。

図１０（ｂ）は、リードイン領域に記録されているコントロールデータ領域のデータ構造を示す。コントロールデータ領域は、物理情報セクタと、スクランブル情報セクタとを含んでいる。物理情報セクタには、ディスク径やディスク構造、

記録密度等のディスクの物理情報が記録されている。スクランブル情報セクタには、情報記録媒体のデータ記録領域に記録されたデータに対して施されたスクランブル方式等の情報が記録されている。スクランブル情報セクタは、情報再生装置が逆スクランブル処理を施すために参照される。なお、スクランブル情報セクタの詳細な内容については、後に図を参照して説明する。

図１０（ｃ）は、ボリューム・ファイル管理領域のデータ構造を示す。本実施の形態では、ボリューム・ファイル管理領域のデータ構造は、国際標準規格ＩＳＯ９６６０（International Standard Organization 9660）に準拠している。この国際標準規格ＩＳＯ９６６０は、ＣＤ－ＲＯＭ（Compact Disc-Read Only Memory）において採用されている。

ボリューム・ファイル管理領域は、ボリューム記述子と、パステーブルと、ディレクトリレコードとを含んでいる。

ボリューム記述子には、ボリューム空間のサイズやパステーブルの記録位置情報、ディレクトリレコードの記録位置情報、ディスク作成日時等の情報が記録されている。パステーブルには、情報記録媒体上に存在する全てのディレクトリのパスと記録位置情報とを対応づけるテーブルが記録されている。ディレクトリレコードには、各ディレクトリまたはファイルの識別子（一般的には、ディレクトリ名又はファイル名）、データの記録位置情報、ファイルのサイズ、属性等の情報が記録されている。

図１０（ｄ）は、ディレクトリレコードの更に詳細なデータ構造を示している

。ルートディレクトリ用ディレクトリレコードには、ルートディレクトリの属性や識別子、作成日時等が記録されている。また、ルートディレクトリ用ディレクトリレコード（第１セクタ）には、ディレクトリの記録位置情報が記録されている。ルートディレクトリ用ディレクトリレコード（第２セクタ）にも、同様な情報が記録されている。また、ファイルＡ用ディレクトリレコードには、ファイルＡのデータの記録位置情報、データ長、ファイルの識別子情報、著作権管理識別子等

が記録されている。このように、複数のディレクトリは階層構造を有している。ルートディレクトリは、その階層構造の最も上位に位置するディレクトリである。これらの更に詳細な内容については後に図を参照して説明する。

データ記録領域には、スクランブルされているファイルと、スクランブルされていないファイルとが記録されている。例えば、スクランブルファイルＡとスクランブルファイルＣとは、スクランブルされているファイルであり、非スクランブルファイルＢは、スクランブルされていないファイルである。著作権保護の対象になっているＡＶデータを格納するファイルは、スクランブルされているファイルであることが好ましい。

図１０（ｃ）は、スクランブルファイルＡのデータ構造を示す。ファイルＡは、セクタｎから連続する複数のセクタに区分されている。複数のセクタのそれぞれに格納されるデータには、スクランブル処理が施されている。以下、本明細書では、スクランブル処理が施されたデータを格納するセクタを「スクランブルセクタ」という。

図１０（ｆ）は、非スクランブルファイルＢのデータ構造を示す。ファイルＢは、セクタｍから連続する複数のセクタに区分されている。複数のセクタのそれぞれに格納されるデータには、スクランブル処理は施されていない。以下、本明細書では、スクランブル処理が施されていないデータを格納するセクタを「非スクランブルセクタ」という。

図１１（ａ）～（ｃ）は、ボリューム・ファイル管理領域中のディレクトリレコードのデータ構造を示す。ディレクトリレコードは、ディレクトリレコード長

と、ファイル記録位置情報と、ファイルデータ長と、ファイル識別子と、著作権管理情報とを含む。

ディレクトリレコード長は、ファイル（又はディレクトリ）のディレクトリレコードのサイズを示す情報である。ファイル記録位置情報は、ファイルのデータが記録されたセクタ（以下、エクステントと称す）の開始位置を示す情報である。

ファイルデータ長は、ファイルを構成するセクタ数を示す情報である。ファイル識別子は、ファイルを識別するための識別情報（ファイル名）である。著作権管理情報は、ファイルの著作権管理に関する情報である。

著作権管理情報は、スクランブルフラグ領域とスクランブル方式領域とを含む。スクランブルフラグ領域には、ファイルのデータにスクランブル処理が施されているか否かを示すフラグが記録される。ファイルのデータにスクランブル処理が施されている場合には、値１を有するフラグがスクランブルフラグ領域に記録され、ファイルのデータにスクランブル処理が施されていない場合には、値０を有するフラグがスクランブルフラグ領域に記録される。従って、スクランブルフラグ領域を参照することにより、ファイルのデータにスクランブル処理が施されているか否かを判定することができる。スクランブル方式領域には、ファイルのデータに施されたスクランブル処理の方式を示す識別子が記録される。従って、スクランブル方式領域を参照することによって、データに施されたスクランブル処理方式をファイル単位に決定することができる。

以下、図１１（ｄ）～（ｆ）を参照して、スクランブル方式の一例を説明する。このスクランブル方式に対応するスクランブル方式識別子を１とする。

図１１（ｄ）は、リードイン領域のコントロールデータ領域に記録されているスクランブル情報セクタのデータ構造を示す。スクランブル情報セクタは、セクタヘッダ領域とメインデータ領域とを含む。

スクランブル情報セクタのセクタヘッダ領域は、情報再生装置がセクタを識別するための識別子が記録されているアドレス領域と、情報記録領域に施されたスクランブル方式を特定するための情報（前記のように、本例のスクランブル方式

を１とする）が記録されたスクランブル方式領域と、情報再生装置が再生データの転送を要求する機器に著作権保護対象のデータを送出して良いか否かを決定するための認証処理（以下、相互認証処理と呼ぶ）に使用する相互認証鍵が記録された相互認証鍵領域とを含む。この相互認証処理については後に詳しく述べる。

スクランブル情報セクタのメインデータ領域には、スクランブルのための鍵からスクランブル処理時に使用する乱数系列を決定するためのテーブルが記録されている。従って、情報再生装置は、スクランブル情報セクタに記録されたテーブルとスクランブルのための鍵とを用いることで初めて、デスクランブル処理が可能となる。ただし、上記の乱数系列を決定する初期値を、以下ではプリセットデータと称する。

図１１（ｃ）は、データ記録領域中のスクランブルセクタのデータ構造を示す。

スクランブルセクタのセクタヘッダ領域は、アドレス領域と、セクタのメインデータ領域にスクランブル処理が施されているか否かを識別するフラグが記録されたスクランブルフラグ領域と、スクランブル時に使用した鍵（以下、シードキーと称す）が記録されたシードキー領域と、ファイルの用途を識別する情報が記録された用途識別情報領域とを含む。スクランブルフラグ領域には、スクランブル処理が施されていることを示す１が記録されており、シードキー領域にはメインデータ領域のデスクランブル処理に用いる鍵が記録されている。また、用途識別情報領域には、業務用、民生用等の記録されたデータの用途についての情報が記録されており、情報再生装置の用途が用途識別情報と異なる場合の再生制限を示す情報が記録されている。また、メインデータ領域には、リードイン領域のスクランブル情報セクタで指定されたスクランブル方式と、スクランブルセクタのセクタヘッダ領域のシードキーとによって決定されるスクランブル処理が施されたデータが記録されている。つまり、シードキー領域に記録された値をもとにスクランブル情報セクタのテーブルを参照してプリセットデータを決定し、そのプリセットデータによって決定される乱数系列を用いてスクランブル／デスクランブル処理が可能となる。以下では、シードキーはファイル毎に同一であるとして

説明を行う。

一方、非スクランブルセクタのセクタヘッダは、アドレス領域とスクランブルフラグ領域を含む。スクランブルフラグ領域には、セクタのメインデータ領域にスクランブル処理が施されていないことを示す0が記録されている。従って、情報再生装置は、スクランブルフラグ領域の値が0であることを検知することにより、デスクランブル処理を施す必要がないことを容易に認識できる。

次に、図12を参照して、スクランブル方式の一例を説明する。

図12（a）は、8ビットのデータ系列D．（jは0から2047までの整数）をある初期値をもとに発生させた8ビットの乱数系列S jと論理演算を行うことにより、スクランブルされたデータSDjが得られることを示す。すなわち、リードイン領域に記録されたスクランブル情報セクタと、各セクタのセクタヘッダ領域のシードキーによって定まる15ビットのプリセットデータをシフトレジスタ301にセットし、上位ビット方向にシフトを行いながら最上位ビットr_{14}とビットr_{11}の排他的論理和をビット0に入れることで乱数系列S jを発生する。ここで、1ビットシフトする度にビット位置r_nのビットを論理演算ブロック302に入力される8ビットの数値をS jとする。以下の様にして得られるS jと8ビットの記録データD jとの論理演算（例えば、排他的論理和など）によってスクランブル後のデータSDjが得られる。1セクタのメインデータのサイズを2048バイトとすると、前記の操作をSD0からSD2047まで2048回繰り返すことで1セクタのスクランブル処理を行うことができる。

また、図12（b）および（c）は、スクランブル情報セクタからプリセットデータを決定するテーブルへの変換を示している。図12（b）に示すスクランブル情報セクタには、テーブルの各エントリが4つ記録されており、各エントリはシードキーとプリセットデータの組から成る。これらの組をテーブル化すれば図12（c）の様なテーブルが得られる。例えば、セクタヘッダに記録されているシードキーが01b（bは2進数であることを意味する）であれば、プリセットデータとして0077h（hは16進数を意味する）を図12（a）のシフトレジスタ301に初期値として設定し、上記のシフト動作および論理演算を施すことで、スクランブル／デスクランブル処理が可能となる。

以上のように、本実施形態の情報記録媒体は、ファイル単位でスクランブルをかけることを可能とするとともに、スクランブルが施されているか否かの情報をファイル管理領域に著作権管理情報として有するとともに、セクタ単位にもセクタヘッダのスクランブルフラグ領域に有することで、パーソナルコンピュータのようにメインデータの認識しか行えない装置にスクランブル処理の有無の認識を可能とし、光ディスクドライブのようなメインデータの認識が行えない装置にもスクランブル処理の有無の認識を可能とする。従って、パーソナルコンピュータに接続された光ディスクドライブによってデータを再生する場合にも、その両者が著作権保護対象のデータであるか否かを判別することを可能とする。

また、本実施の形態の情報記録媒体は、シードキーを変更することによってファイル毎に異なるスクランブル処理を施すことができるため、仮に不正行為によって一つのスクランブルファイルのスクランブル方法を解読されたとしても、解読されたスクランブル方式で他のスクランブルファイルをデスクランブルすることを防止することができ、著作権保護処理を行う上でのセキュリティを向上することが可能となる。

また、本実施の形態の情報記録媒体を著作権保護目的で使用する場合には、デスクランブルに必要不可欠なスクランブル情報を記録したスクランブル情報セクタが、パーソナルコンピュータのような機器からは読み出すことのできないリードイン領域に存在しているために、スクランブル情報を不正に読みだそうとする行為を防止する効果が高い。また、リードイン領域はデータ記録領域と同一の再生手段で再生可能なために、特別な再生手段を新たに設ける必要がない。

また、セクタ単位に記録した、シードキー、スクランブルフラグ、用途識別情報等の情報を、パーソナルコンピュータのような機器からは読み出すことのできないセクタヘッダ領域に記録しているために、前記のリードイン領域にスクランブル情報を記録するのと同様に、不正に前記情報を読み出そうとする行為を防止

する効果がある。

また、セクタヘッダ領域に用途識別情報を記録しているために、記録されたデータの内容に応じて再生装置が再生を行うべきか、再生を禁止すべきかの判定を行うことを可能とする。よって、例えば、業務用のディスクと民生用のディスクとで本領域に異なる識別子を記録することで、民生用再生装置で業務用ディスクが再生することを防止できる。

また、相互認証処理に用いる相互認証鍵を記録することで、再生装置が相互認証動作で送受信するデータを該相互認証鍵毎に変更することが可能となり、相互認証処理の処理方法を不当に解読することを防止する効果がある。従って、相互認証処理を不当に行って、磁気ディスクドライブなどに不当にコピー動作を行おうとする行為を防止することが可能となる。

なお、本実施の形態において、ボリューム・ファイル構造は国際規格であるＩＳＯ９６６０をもとにしたが、本発明に述べたような情報を有するボリューム・ファイル構造であればこれに限らないことは言うまでもない。

なお、本実施の形態において、スクランブル方式は乱数とデータの論理演算を用いるとしたが、本実施の形態のようにテーブルとテーブルを参照するためのシードキーを有するスクランブル方式であればこれに限らないことは言うまでもない。

なお、本実施の形態において、リードイン領域にはプリセットデータを決定するためのテーブルを記録したが、テーブルを決定するためのパラメータであればこれに限らず、あらかじめ既知の複数のテーブルからただ一つのテーブルを特定するための識別子を記録しても良い。

なお、本実施の形態において、スクランブルセクタのセクタヘッダ領域に用途識別情報領域として用途識別のための情報記録領域を確保したが、明確に分離した領域として確保しなくても、シードキーの値によって用途を分類するようにしても良いことは言うまでもない。

なお、本実施の形態において、スクランブルセクタはメインデータ領域の２０４８バイト全てにスクランブル処理が施されていることとしたが、メインデータ領域の全てにスクランブル処理が施されていなくとも、定められた一部の領域のみにスクランブル処理が施されていても良い。

〔第４の実施形態〕

次に、本発明に係る情報記録媒体の他のデータ構造を説明する。情報記録媒体のデータ構造は、図１０に示される情報記録媒体の構造と同様である。ここでは、図１０に示されるデータ構造と異なる点についてのみ説明する。

図１３（ａ）～（ｃ）は、ボリューム・ファイル管理領域に記録されたディレクトリレコードのデータ構造を示す。ディレクトリレコードの著作権管理情報中のスクランブル方式領域には、本実施の形態で説明するスクランブル方式を示す２が記録されている。

図１３（ｃ）は、スクランブルセクタのデータ構造を示している。スクランブルセクタのセクタヘッダ領域は、アドレス領域と、スクランブルフラグ領域と、メディアＣＧＭＳ（Copy Generation Management System）データ領域と、暗号化オリジナルＣＧＭＳデータ領域と、暗号化タイトル鍵領域と、暗号化用途識別情報領域とを含む。

スクランブルフラグ領域には、スクランブル処理が施されていることを示す１が記録されている。

メディアＣＧＭＳデータ領域には、情報記録媒体のコピー許可情報が記録されている。暗号化オリジナルＣＧＭＳデータ領域には、本セクタのデータが他の媒体からコピーされている場合において、最もオリジナルのデータのコピー許可情報が記録されている。ここで、メディアＣＧＭＳデータは、情報記録媒体のデータのコピー許可情報を表す。メディアＣＧＭＳデータは、コピー動作時に更新される。オリジナルＣＧＭＳデータは、ディスク作成時のコピー許可情報を表す。

オリジナルＣＧＭＳデータは、暗号化が施されているために、コピー動作時もそのままコピーされる。（表１）にメディアＣＧＭＳデータ、オリジナルＣＧＭＳデータの定義を示す。

表1

メディアCGMSデータ／オリジナルCGMSデータ	内容
00b	コピー許可
01b	未使用
10b	1回コピーのみ許可
11b	コピー禁止

（表1）から、例えば、メディアCGMSデータが11bであって、オリジナルCGMSデータが10bであったとすれば、そのセクタのデータは、もともと1回のみコピー許可状態（メディアCGMSデータおよびオリジナルCGMSデータがともに01b）であって、既に1回のコピー動作が行われたことによってメディアCGMSデータがコピー禁止を意味する11bに変更されたと判定すべきである。以下では、メディアCGMSデータと、オリジナルCGMSデータを合わせてCGMS制御情報と称する。

暗号化タイトル鍵領域には、メインデータ領域に施されたスクランブル処理をデスクランブルするための鍵が記録されている。

暗号化用途識別情報領域には、用途を指定するための識別情報が暗号化されて記録されている。ただし、前記の暗号化オリジナルCGMSデータ領域、暗号化タイトル鍵領域、暗号化用途識別情報領域はいずれも暗号化処理が施されており、セクタヘッダ領域を読み出しただけでは情報を得ることはできない。これらの暗号化データは情報記録媒体のリードイン領域のセクタヘッダ領域に記録された暗号化ディスク鍵を用いて暗号化されている。したがって、スクランブル情報セクタのヘッダ領域の暗号化情報を復号するためには、前記暗号化ディスク鍵が必要となる。

図13（d）は、スクランブル情報セクタのデータ構造を示す。以下の説明では、暗号化されたデータと暗号を復号化したデータとを明確に区別するため、暗号化されたデータは「暗号化」をつけた名称で表すこととし、暗号を復号化したデータは「復号化」をつけた名称で表すこととする。例えば、タイトル鍵を暗号化することによって得られるデータは「暗号化タイトル鍵」といい、暗号化タイトル鍵を復号化することによって得られるデータは「復号化タイトル鍵」という。

スクランブル情報セクタは、リードイン領域のコントロールデータ領域に記録されている。

スクランブル情報セクタのセクタヘッダ領域には、スクランブル方式が本方式のスクランブル方式であることを示す2が記録されている。また、相互認証鍵領域には、デスクランブル後のデータを送出するか否かを決定するための相互認証処理に用いられる相互認証鍵が記録されている。本相互認証鍵については、後述する情報再生装置の実施形態において、詳しく述べることとする。

スクランブル情報セクタのメインデータ領域には、スクランブルセクタの暗号化オリジナルCGMSデータ、暗号化タイトル鍵、暗号化用途識別情報を復号するための暗号化ディスク鍵が記録されている。ただし、暗号化ディスク鍵はさらに暗号化が施されており、暗号化ディスク鍵を復号するための鍵（以下、マスター鍵と称す）は、情報再生装置によって提供される。

スクランブル情報セクタのメインデータ領域には、暗号化ディスク鍵1、暗号化ディスク鍵2、・・・と複数の暗号化ディスク鍵が記録されており、暗号化ディスク鍵1はマスター鍵1で、暗号化ディスク鍵2はマスター鍵2で、・・・というようにそれぞれ対応したマスター鍵によって暗号化されている。ここで、暗号化ディスク鍵1、暗号化ディスク鍵2、・・・は、同一のディスク鍵情報を異なるマスター鍵で暗号化したものである。従って、ある情報再生装置Aがマスター鍵1を内部に有しており、別の情報再生装置Bがマスター鍵2を内部に有している場合、情報再生装置Aは暗号化ディスク鍵1を、情報再生装置Bは暗号化ディスク鍵2をそれぞれ復号して、同一の内容の復号化ディスク鍵を得ることが可能となる。

図13（f）は、非スクランブルセクタのデータ構造を示す。スクランブルセクタフラグ領域には0が記録されている。メインデータ領域に記録されているデ

ータにはスクランブル処理が施されていない。このことは、従来の情報記録ディスクと同様なデータアクセスが可能であることを示している。

以上のように、本実施形態の情報記録媒体は、非スクランブルセクタの再生に際しては従来と全く同様のアクセスでのデータ再生が可能である。一方、スクランブルセクタの再生を行うためには、マスター鍵を有する情報再生装置が、リードイン領域のスクランブル情報セクタを読み出して暗号化ディスク鍵をマスター鍵で復号し、さらに、復号化したディスク鍵を用いてスクランブルセクタのセクタヘッダの暗号化タイトル鍵を復号化し、復号化したタイトル鍵を用いてスクランブルデータのデスクランブル処理を行うことでデータの再生が可能となる。

以下では、スクランブル方式の例として、第３の実施形態で述べたスクランブル方式を用いる場合について述べる。第３の実施形態においては、変換テーブルを用いてプリセットデータを生成したが、本実施形態の情報記録媒体では、暗号化タイトル鍵領域に乱数発生のための初期値を暗号化して記録すれば、図１２（ａ）のシフトレジスタ３０１と論理演算ブロック３０２とを用いて容易にデータのスクランブル処理が行える。すなわち、復号したタイトル鍵をシフトレジスタ３０２の初期値とし、シフトを繰り返すことで乱数系列Ｓ を発生し、データ系列Ｄ との論理演算をとることにより、スクランブル処理が可能となる。また、図１２（ａ）のシフトレジスタ３０１を用いて、データのデスクランブルも同様に可能となる。

以上のように、本実施の形態の情報記録媒体は、ファイル単位でスクランブル

をかけることを可能とするとともに、スクランブルが施されているか否かの情報をファイル管理領域に著作権管理情報として有するとともに、セクタ単位にもセクタヘッダのスクランブルフラグ領域に有することで、パーソナルコンピュータのようにメインデータの認識しか行えない装置にスクランブル処理の有無の認識を可能とし、光ディスクドライブのようなメインデータの認識が行えない装置にもスクランブル処理の有無の認識を可能とする。従って、パーソナルコンピュータに接続された光ディスクドライブによってデータを再生する場合にも、その両者が著作権保護対象のデータであるか否かを判別することを可能とする。

また、本実施の形態の情報記録媒体は、タイトル鍵を変更することによってファイル毎に異なるスクランブル処理を施すことができるため、仮に不正行為によって一つのスクランブルファイルのスクランブル方式を解読されたとしても、解読されたスクランブル方式で他のスクランブルファイルをデスクランブルすることを防止することができ、著作権保護処理を行う上でのセキュリティを向上することが可能となる。

また、本実施の形態の情報記録媒体を著作権保護目的で使用する場合には、デスクランブルに必要不可欠なスクランブル情報を記録したスクランブル情報セクタが、パーソナルコンピュータのような機器からは読み出すことのできないリードイン領域に存在しているために、スクランブル情報を不正に読みだそうとする行為を防止する効果が高い。また、リードイン領域はデータ記録領域と同一の再生手段で再生可能なために、特別な再生手段を新たに設ける必要がない。

また、セクタ単位に記録した、スクランブルフラグ、ＣＧＭＳ制御情報、暗号化タイトル鍵、暗号化用途識別情報を、パーソナルコンピュータのような機器からは読み出すことのできないセクタヘッダ領域に記録しているために、前記のリードイン領域にスクランブル情報を記録するのと同様に、不正に前記セクタヘッダ中の情報を読み出そうとする行為を防止する効果がある。

また、セクタヘッダ領域に用途識別情報を記録しているために、記録されたデータの内容に応じて再生装置が再生を行うべきか、再生を禁止すべきかの判定を行うことを可能とする。よって、例えば、業務用のディスクと民生用のディスクとで本領域に異なる識別子を記録することで、民生用再生装置で業務用ディスクが再生することを防止できる。

また、相互認証処理に用いる相互認証鍵を記録することで、再生装置が相互認証動作で送受信するデータを該相互認証鍵毎に変更することが可能となり、相互認証処理の処理方法を不当に解読することを防止する効果がある。従って、相互認証処理を不当に行って、磁気ディスクドライブなどに不当にコピー動作を行おうとする行為を防止することが可能となる。

また、本実施の形態の情報記録媒体は、スクランブルセクタのメインデータを

タイトル鍵で暗号化し、タイトル鍵をディスク鍵で暗号化し、ディスク鍵をマスター鍵で暗号化するという階層的な暗号化／スクランブル処理を施しているために、不正にスクランブルセクタのメインデータをコピーされた場合でも、そのデスクランブルを防止する効果があるため、不正コピーを無意味なものとする事が可能である。

また、ＣＧＭＳ制御情報を記録しているために、本実施の形態の情報記録媒体から他の書き換え型媒体にファイルコピーされた場合にも、不正コピーされたか、正規コピーされたかを判定することを可能とする。

なお、本実施の形態ではタイトル鍵を初期値とした乱数とデータとの論理演算によってスクランブル処理を行う例を示したが、スクランブル方式はこれに限らず、指定された鍵に応じてデータをスクランブルする方式であれば他のスクランブル方式でも良いことは言うまでもない。

なお、本実施の形態のボリューム・ファイル構造は、国際標準規格であるＩＳＯ９６６０をもとに説明したが、本実施の形態で述べた内容と同等の著作権管理情報を記録できるボリューム・ファイル構造であれば、これに限らないことは言うまでもない。

なお、本実施の形態において、スクランブルセクタはセクタの全てのデータがスクランブルされているとしたが、セクタのメインデータ全域がスクランブルされていなくとも、メインデータの一部のみがスクランブルされていても良いことは言うまでもない。

なお、本実施の形態において、スクランブルファイルではファイルを構成する全てのセクタにスクランブルが処理が施されているとしたが、スクランブルファイルの一部のセクタのみにスクランブル処理が施されていても良いことは言うまでもない。

なお、本実施の形態において、ＣＧＭＳ制御情報は、１回コピーのみ許可、コピー禁止、コピー許可の３種のみを用いていたが、割り当てるビットを拡張することで容易に２回コピー許可、３回コピー許可などの情報を記録できることは言うまでもない。

なお、本実施の形態で述べたメインデータのスクランブル方法は一例であり、ある鍵情報（本実施の形態ではタイトル鍵）をもとにスクランブルする方法であれば、これに限らない。

（第５の実施形態）

以下、図面を参照しながら、本発明に係る情報記録媒体を再生するための情報再生装置を説明する。特に断らない限り、情報再生装置は、本発明に係る情報記録媒体の第３の実施の形態と第４の実施の形態に共通して再生可能な装置であることとする。従って、以下では情報記録媒体の第４の実施の形態を再生する場合の動作を例に説明するが、暗号化タイトル鍵領域をシードキー領域と、スクランブル情報セクタの暗号化ディスク鍵をプリセットデータ変換テーブルと、それぞれ置き換えることによって情報記録媒体の第３の実施の形態についても同様に処理できる。

図１４は、本発明に係る情報再生装置５００の構成をボナブロック図である。

情報再生装置５００は、メインプロセッサ５０１と、バスインタフェース回路５０３と、主記憶５０４と、ＳＣＳＩ（Small Computer System Interface）で定められるプロトコルを制御するＳＣＳＩ制御カード５０６と、圧縮されたディジタルＡＶデータを伸張してアナログＡＶデータに変換して出力するＡＶデコーダカード５０７と、本発明に係る情報記録媒体を再生する光ディスクドライブ５０９と、ハードディスクドライブ５１０とを含んでいる。

メインプロセッサ５０１と、バスインタフェース回路５０３と、主記憶５０４とは、プロセッサバス５０２を介して相互に接続されている。バスインタフェース回路５０３と、ＳＣＳＩ制御カード５０６と、ＡＶデコーダカード５０７とは、システムバス５０５を介して、相互に接続されている。ＳＣＳＩ制御カード５０６と、光ディスクドライブ５０９と、ハードディスクドライブ５１０とは、ＳＣＳＩバスを介して、相互に接続されている。

次に、情報再生装置５００によるＡＶファイルの再生動作について説明する。

光ディスクドライブ５０９に光ディスクが装着されると、メインプロセッサ５０１は、ＳＣＳＩ制御カード５０６を介して前記光ディスクのボリューム・ファ

イル管理領域を読み出し、主記憶５０４に格納する（以下、格納したボリューム・ファイル管理領域のデータをファイル管理情報と称す）。

メインプロセッサ５０１は、ＡＶデコーダカード５０７と光ディスクドライブ５０９との間で互いの機器が著作権保護機能を有する機器であるか否かを判定する処理（以下、相互認証処理と称す）を行う。その処理過程においていずれかの機器からエラーを検出した場合には相互認証処理が失敗したとみなし、以下の処理を中止する。一方、相互認証処理が正常に終了した場合に光ディスクドライブ５０９は、装着されたディスクの暗号化ディスク鍵をＡＶデコーダカードに転送する。この際、光ディスクドライブ５０９は、暗号化ディスク鍵の出力時に、さらに相互認証処理中に生成した鍵（以下、バス鍵と称す）に基づいて暗号化を施した暗号化ディスク鍵を送出する。ＡＶデコーダカード５０７は受け取った暗号化ディスク鍵を、バス鍵で復号化を行った後、内部で保持する。

その後、光ディスクに記録されたファイルを再生する場合にメインプロセッサ５０１は、あらかじめ主記憶５０４に格納したファイル管理情報中の著作権管理情報のスクランブルフラグを参照し、再生を行うファイルがスクランブルされたファイルであるか否かを判定する。判定の結果、再生するファイルがスクランブルされていないファイルであると判定されれば、光ディスクドライブ５０９はメインプロセッサ５０１からＳＣＳＩ制御カード５０６を介して再生命令を受領し、非スクランブルデータを転送する。一方、メインプロセッサ５０１がファイル管理情報のスクランブルフラグからスクランブルされたファイルであると判定すれば、再び光ディスクドライブ５０９とＡＶデコーダカード５０７間の相互認証処理を実行する。

メインプロセッサ５０１は、相互認証処理中にエラーを検出すれば、再生処理を行わずに処理を中止する。一方、相互認証処理が正常に終了した場合には、データの再生に先だって、光ディスクドライブ５０９は暗号化タイトル鍵を返送し、メインプロセッサ５０１によってＡＶデコーダカード５０７に転送される。この時、光ディスクドライブ５０９はあらかじめ保持しているバス鍵によって暗号化した暗号化タイトル鍵を転送する。また、ＡＶデコーダカード５０７は受け取った暗号化タイトル鍵を、バス鍵で復号化した後に内部的に格納する。

その後、光ディスクドライブ５０９は装着されたディスクから読み出されるスクランブルデータを送出し、マイクロプロセッサ５０１は該スクランブルデータをＡＶデコーダカード５０７に転送する。ＡＶデコーダカード５０７は、既に内部に格納するタイトル鍵に用いて、受信したスクランブルデータをデスクランブルし、アナログＡＶデータに変換し、ビデオ出力、オーディオ出力からアナログ信号として出力する。以上のようにして、情報再生装置５００は、本発明の情報記録媒体を再生することが可能となる。

光ディスクドライブ５０９からハードディスクドライブ５１０へのスクランブルファイルのコピー動作については、ハードディスクドライブ５１０が相互認証処理を実行できないために、相互認証処理がエラー終了となる。従って、光ディスクドライブ５０９がデータをＳＣＳＩバスに送出する前に処理は中止され、コピー動作は実行されない。

また、仮に、光ディスクドライブ５０９が読み出したスクランブルファイルを不当にハードディスクドライブ５１０へコピーするためのプログラムが主記憶５０４にロードされ、何らかの形で相互認証処理を正常終了させた後に、転送されたスクランブルデータをハードディスクドライブ５１０にコピーした場合には、スクランブルデータはハードディスクドライブ５１０にコピーされる。しかしながら、ハードディスクドライブ５１０にコピーされたデータを再生するためには、再びハードディスク５１０とＡＶデコーダカード５０７の相互認証処理が必要となり、この場合にハードディスクドライブ５１０はバス鍵を生成する手段を持たないために、ハードディスク５１０上のスクランブルファイルがＡＶデコーダカード５０７によって再生されることは不可能となる。

従って、不正なコピーが仮になされたとしても、そのコピー動作を無意味なものとすることができ、結果として著作権保護機構を実現することができる。

以下に、情報再生装置５００の構成要素である光ディスクドライブ５０９およびＡＶデコーダカード５０７の更に詳細な構成および動作について、それぞれ図１５、図１６を参照して説明する。

図１５は、光ディスクドライブ５０９の構成を示すブロック図である。以下にその構成について説明する。６００はＳＣＳＩ制御回路を、６０１はＡＶデコーダとの相互認証処理を行うためのデコーダ認証回路を、６０２は光ディスクドライブ全体を制御するマイクロコントローラを、６０３はマイクロコントローラの動作プログラムを格納したプログラムＲＯＭを、６０４は制御データを伝送する制御バスを、６０５はデータの再生時に、読み出しエラーを訂正するためのエラー訂正処理時に使用されるＥＣＣ（Error Correction Code）処理用メモリを、

６０６は光ディスク６０７からのデータの読み出し、２値化、復調、エラー訂正処理等を行うデータ再生回路を、６０７は本発明に係る情報記録媒体であって、前記第３の実施の形態又は第４の実施の形態に示されるデータ構造を有する光ディスクを、それぞれ示している。

次に、光ディスクドライブ５０９の動作について、相互認証処理時およびデータ再生時の動作について述べる。

相互認証処理要求をＳＣＳＩ制御回路６００によって受け取った光ディスクドライブ５０９は、デコーダ認証回路６０１を制御して定められた相互認証処理を実行する。本プロトコルについては、後に詳しく述べるためここでは省略する。前記相互認証処理のプロトコルにおいて、マイクロコントローラ６０２が何らかのエラーを検出した場合には、ＳＣＳＩ制御回路６００からエラーを報告して相互認証処理およびそれに続く鍵情報転送動作を中止する。正常に相互認証処理が終了した場合には、デコーダ認証回路６０１には相互認証処理時に決定されるバス鍵が格納される。

相互認証処理がディスク交換時やリセット時のものであれば、相互認証処理に引き続いて暗号化ディスク鍵の読み出し要求が光ディスクドライブ５０９に発行される。この時、光ディスクドライブ５０９は、データ再生回路６０６を制御して光ディスク６０７から暗号化ディスク鍵情報を読み出し、さらにデコーダ認証回路６０１で既に保持しているバス鍵を使用して暗号化を施した暗号化ディスク鍵をＳＣＳＩ制御回路６００から送出する。一方、スクランブルファイルの再生時における相互認証処理であった場合は、相互認証処理の正常終了に引き続いて

、暗号化タイトル鍵の読み出し命令を光ディスクドライブ５０９は受領する。この時光ディスクドライブ５０９は、データ再生回路６０６を制御して光ディスク６０７から暗号化タイトル鍵情報を読み出し、さらにデコーダ認証回路６０１で既に保持しているバス鍵を使用して暗号化を施したデータをＳＣＳＩ制御回路６００から送出する。

その後に発行されるファイルデータの再生要求に対して光ディスクドライブ５０９は、光ディスク６０７から読み出したスクランブルデータをＳＣＳＩ制御回路６００から送出する。以上で光ディスクドライブ５０９の説明を終わる。

なお、本実施の形態の光ディスクドライブ５０９は、暗号化ディスク鍵の転送要求を受領してから、光ディスク６０７の暗号化ディスク鍵領域を再生するとしたが、光ディスク６０７装着時に読み込んで、内部的に保持していても良いことは言うまでもない。

次に、ＡＶデコーダボードの構成および動作について図１６を参照して説明する。

図１６は、ＡＶデコーダカード５０７の構成を示すブロック図である。以下にその構成要素について説明する。７００はシステムバスと情報の送受信を制御するシステムインタフェース回路を、７０１は光ディスクドライブ５０９と相互認証処理を行うドライブ認証回路を、７０２はＡＶデコーダカード５０７全体を制御するマイクロコントローラを、７０３はマイクロコントローラ７０２の動作プログラムを格納したプログラムＲＯＭを、７０４は制御情報を伝送する制御バスを、７０５はスクランブルデータをデスクランブルするためのデスクランブル回路を、７０６は圧縮されたディジタルＡＶデータを伸張してアナログＡＶデータに変換するオーディオ／ビデオデコーダ回路を、７０７はオーディオ／ビデオデコーダ回路７０６がデータ変換に使用する作業用メモリであるオーディオ／ビデオデコード用メモリを、それぞれ示している。

次にＡＶデコーダカード５０７の動作について、相互認証処理時およびスクランブルファイル再生時の動作について説明する。

まずリセット時やメディア交換時における相互認証処理時には、マイクロコン

トローラ７０２はドライブ認証回路７０１を制御して光ディスクドライブ５０９と所定のプロトコルに従って相互認証処理を実行する。前記相互認証処理中にドライブ認証回路７０１が何らかのエラーを検出した場合には、システムインタフェース回路７００を介してエラーを報告し、処理を打ち切る。一方、正常に相互認証処理が終了した場合にドライブ認証回路７０１は相互認証処理で決定したバス鍵を内部的に保持する。

さらに、ＡＶデコーダカード５０７は、システムインタフェース回路７００から暗号化ディスク鍵を受け取る。ここで、受領した暗号化ディスク鍵は光ディスクドライブ５０９においてバス鍵を用いて暗号化されているため、ＡＶデコーダカード５０７はドライブ認証回路７０１において既に保持するバス鍵で復号化した後にデスクランブル回路７０５に転送する。デスクランブル回路７０５内は受け取った暗号化ディスク鍵を、内部に格納する。

一方、スクランブルファイルの再生時には、ファイルの再生に先だって再び光ディスクドライブ５０９との相互認証処理が実行される。ここでも相互認証処理においてエラーが発生した場合には相互認証処理およびそれに続くファイル再生動作を中止する。相互認証処理がエラーなく正常に終了した場合にＡＶデコーダカード５０７は、システムインタフェース回路７００を介して暗号化タイトル鍵を受信する。暗号化タイトル鍵は光ディスクドライブ５０９において、バス鍵を用いて更に暗号化されているために、ドライブ認証回路７０１において保持しているバス鍵によって復号され、デスクランブル回路７０５に転送される。デスクランブル回路７０５内は、受領した暗号化タイトル鍵を内部的に格納する。

その後、システムインタフェース回路７００から受信するスクランブルファイルのスクランブルデータはそのままデスクランブル回路７０５に転送され、既に保持しているタイトル鍵をもとにデスクランブル処理が行われ、オーディオ／ビデオデコード回路７０６に転送されてアナログＡＶ信号に変換されて出力される。

以上のように、本実施の形態の情報再生装置５００によれば、内部の光ディスクドライブ５０９にデコーダ認証回路６０１、ＡＶデコーダカード５０７にドライブ認証回路７０１をそれぞれ有しているために、ファイルを不正にコピーする目的の機器には鍵情報を送出しない。したがって、仮にスクランブルファイルのデータが不正にコピーされたとしても、そのデスクランブルを実行するための鍵情報を送出しないことで、コピーデータを無意味なものとすることができる。従って、ファイルの著作権を保護する効果がある。

また、本実施の形態の情報再生装置によれば、ＡＶデコーダカード５０７内に鍵情報に応じたデスクランブル処理を施すデスクランブル回路７０５を有するために、スクランブルされたデータをデスクランブルして再生することが可能である。

なお、本実施の形態では、光ディスクドライブ５０９が接続されるバスをＳＣＳＩバスであるとしたが、定められたプロトコルに従って再生データが転送できればこれに限らず、ＡＴＡＰＩ（ＡＴ Attachment Packet Interface）やＩＥＥＥ１３９４（Institute of Electrical and Electronics Engineers 1394）等に従ったバスであっても良いことは言うまでもない。

なお、本実施の形態において、デコーダ認証回路６０１の機能およびドライブ認証回路７０１の機能は、マイクロコントローラ６０２および７０２によって実行されるソフトウェアによって実現されてもよい。

（第６の実施形態）

次に、本発明に係る情報再生装置８００を説明する。

図１７は、本発明に係る情報再生装置８００の構成をボブロック図である。情報再生装置８００の構成は、ＡＶデコーダカード８０１がＳＣＳＩ方式に従って通信を行うためのＳＣＳＩ制御回路を内蔵している点を除いて、図１４にボす情報再生装置５００の構成と同様である。従って、同一の構成要素には同一の参照番号を付し、その説明を省略する。

次に、情報再生装置８００の動作を説明する。

ＳＣＳＩ制御回路内蔵ＡＶデコーダカード８０１は内部にＳＣＳＩ制御回路を内蔵しているため、メインプロセッサ５０１から光ディスクドライブ５０９のス

クランブルファイル再生要求が発行されると、ＳＣＳＩ制御回路内蔵ＡＶデコーダカード８０１と光ディスクドライブ５０９との間で相互認証処理が直接実行される。すなわち、ＳＣＳＩ制御回路内蔵ＡＶデコーダカード８０１が光ディスクドライブ５０９に相互認証のためのコマンドシーケンスを発行し、光ディスクドライブ５０９がそのコマンドに応答することで相互認証処理を行う。

また、データの再生動作においても同様に、光ディスクドライブ５０９に再生要求を行うのは、ＳＣＳＩ制御回路内蔵ＡＶデコーダカード８０１であって、メインプロセッサ５０１ではない。従って、光ディスクドライブ５０９が読み出したデータは直接ＳＣＳＩ制御回路内蔵ＡＶデコーダカード８０１に入力され、アナログＡＶ信号に変換されて出力される。

図１８は、ＳＣＳＩ制御回路内蔵ＡＶデコーダカード８０１の構成を示すブロック図である。以下では、図１６に示したＡＶデコーダカード５０７の構成と異なる点についてのみ説明する。

９００はＳＣＳＩバスとの送受信を制御するＳＣＳＩ制御回路を、９０１はマイクロコントローラによって実行されるプログラムを格納したプログラムＲＯＭを、それぞれ示している。

システムインタフェース回路７００にスクランブルファイルの再生要求が入力されれば、マイクロコントローラ７０２はドライブ認証回路７０１およびＳＣＳＩ制御回路９００を制御して、光ディスクドライブ５０９との相互認証処理を実行する。このとき、相互認証プロトコルは、光ディスクドライブ５０９に対してＳＣＳＩ制御回路９００から直接コマンドが発行される。また、マイクロコントローラ７０２は相互認証プロトコルに従ってドライブ認証回路７０１を制御して相互認証処理を行う。以上の相互認証処理がエラーで終了した場合には、マイクロコントローラ７０２はシステムインタフェース回路７００を制御して、メインプロセッサ５０１にエラーを報告して処理を終了する。一方、相互認証処理が正常に終了した場合には、光ディスクドライブ５０９から直接ＳＣＳＩ制御回路９００によってスクランブルファイルのデータを受け取り、デスクランブル回路７０５でデスクランブルしたデータをオーディオ／ビデオデコーダ回路７０６でアナログＡＶ信号に変換して出力する。以上により、第５の実施の形態の情報再生装置と同様に、本発明の情報記録媒体に記録されたデータの著作権を侵害するコピー動作を防止して、ＡＶデータを再生することが可能となる。

以上のように、本実施の形態の情報再生装置８００では、第５の実施の形態の情報再生装置の特徴に加えて、光ディスクドライブ５０９とＳＣＳＩ制御回路内蔵ＡＶデコーダカード８０１が直接コマンドおよびデータの送受信を行うために、相互認証方式や鍵情報を不当に解読されること、および、ソフトウェアによって不当なコピー動作が実行されることに対するセキュリティが向上する。

なお、再生する情報記録媒体を本発明に係る情報記録媒体の第４の実施の形態を用いて説明したが、本発明に係る情報記録媒体の第３の実施の形態においても全く同様に処理することが可能であり、説明中の暗号化タイトル鍵をシードキーとし、暗号化ディスク鍵をスクランブル情報セクタの変換テーブル情報に置き換えれば良い。

なお、本実施の形態では、光ディスクドライブ５０９が接続されるバスをＳＣＳＩバスであるとしたが、定められたプロトコルに従って再生データが転送できれはこれに限らず、ＡＴＡＰＩ、ＩＥＥＥ１３９４等のインタフェースでも良い。

（第７の実施形態）

次に、本発明に係る情報再生装置１０００を説明する。

図１９は、本発明に係る情報再生装置１０００の構成を示すブロック図である。情報再生装置１０００は光ディスクプレーヤである。情報再生装置１０００の構成要素は、プログラムＲＯＭ１００１を除いて、図１４の情報再生装置の構成要素または図１７の情報再生装置の構成要素と同一である。従って、同一の構成要素には同一の参照番号を付し、その説明を省略する。また、ここでは本発明の情

報記録媒体の第４の実施の形態をもとに説明する。

光ディスクプレーヤ１０００のリセット時又はディスク挿入時に、マイクロコントローラ７０２は、データ再生回路６０６を制御して、光ディスクのリードイ

ン領域のスクランブル情報セクタの読み出しを行う。スクランブル情報セクタから読み出された暗号化ディスク鍵情報はデスクランブル回路７０５に転送されて、内部的に保持される。

一方、光ディスク６０７に記録されたスクランブルファイルを再生する際に、マイクロコントローラ７０２はデータ再生回路６０６を制御して、再生するスクランブルファイルのセクタヘッダ領域から暗号化タイトル鍵を読み出し、デスクランブル回路７０５に転送する。デスクランブル回路７０５は受け取ったタイトル鍵を内部に格納するとともに、用途識別情報の判定を行う。デスクランブル回路７０５は、用途識別情報を判定した結果、再生が禁止されていると判定した場合には、マイクロコントローラ７０２にエラーの発生を報告する。一方、デスクランブル回路７０５が再生が許可されていると判定した場合には、データ再生回路６０６はスクランブルファイルのデータを読み出し、読み出したスクランブルデータをデスクランブル回路７０５に転送する。デスクランブル回路７０５は、あらかじめ格納したディスク鍵およびタイトル鍵を用いてスクランブルデータをデスクランブルし、オーディオ／ビデオデコーダ回路７０６に転送する。オーディオ／ビデオデコーダ回路７０６は受け取ったデータをアナログＡＶ信号に変換して、音声出力／映像出力する。

以上のようにして、光ディスクプレーヤ１０００は、スクランブルデータをデスクランブルして再生することが可能である。ただし、本発明に係る情報再生装置の第５および第６の実施の形態とは異なり、光ディスクプレーヤ１０００は相互認証処理を実行せずに映像再生を行う。これは、本実施の形態においては、再生されたデータが直接オーディオ／ビデオデコーダ回路７０６に入力されるため、途中でハードディスクドライブなどの他の書き換え型メディアへのコピー動作が

不可能であり、相互認証処理が不要であることによる。したがって、本実施の形態の構成には、相互認証処理を実行する構成要素が存在しなくとも、著作権保護が可能となる。また、光ディスクプレーヤ１０００は再生時に用途識別情報の判定を行うために、再生が禁止されている用途のデータを再生することを防止できる。

以下に、本発明に係る情報再生装置の第５の実施の形態および第６の実施の形態において使用される、デコーダ認証回路６０１、ドライブ認証回路７０１、デスクランブル回路７０５の更に詳細な構成および動作を説明する。ただし、以下で述べる構成については、本発明の情報再生装置の第５の実施の形態、第６の実施の形態および第７の実施の形態に共通の構成となっている。

先ず、デスクランブル回路７０５の構成と動作についてを図面を参照して説明する。ただし、デスクランブル回路７０５は、スクランブル方式と深く関係するために、本発明の情報記録媒体の第３の実施の形態を再生する場合と第４の実施の形態を再生する場合とで異なる構成となる。従って以下では、本発明の情報記録媒体の第３の実施の形態を再生するためのデスクランブル回路を図２０および図２１を用いて、本発明の情報記録媒体の第４の実施の形態を再生するためのデスクランブル回路を図２２および図２３を用いて、それぞれ独立に説明する。

図２０は、本発明の情報記録媒体の第３の実施の形態を再生するためのデスクランブル回路１１０６の構成を示すブロック図である。以下、各構成要素について説明する。１１００は制御バス７０４との通信を行うためのＩ／Ｏ制御回路を、１１０１は入力されるデータの内容に応じて出力先のブロックを切り替えるセレクタを、１１０２は再生フィルの用途識別情報を参照して再生許可であるか否かを判定する用途識別回路を、１１０３はシードキーから乱数発生回路１１０４のためのプリセットデータを生成する変換テーブルを格納しておくための変換テーブル記憶回路を、１１０４は前記変換テーブル記憶回路１１０３から出力されるプリセットデータをもとに乱数を発生させる乱数発生回路を、１１０５は乱数発

生回路１１０４で発生された乱数とセレクタ１１０１から入力されるスクランブルデータとの論理演算を行うことによりデスクランブル処理を行うメインデータデスクランブル回路を、それぞれ示している。

次に、デスクランブル回路１１０６の動作を説明する。

まず、相互認証処理が正常に終了した後にリードイン領域に記録されたスクラ

ンブル情報セクタを読み出す場合、Ｉ／Ｏ制御回路１１００を介してセレクタ１１０１にスクランブル情報セクタ読み出し設定がなされ、セレクタ１１０１は出力先を変換テーブル記憶回路１１０３に設定する。入力された読み出しデータはセレクタ１１０１を介して変換テーブル記憶回路１１０３に入力され、乱数発生の初期値となるプリセットデータを決定する変換テーブルとして格納される。

一方、スクランブルファイルの再生時には、データの再生に先立って相互認証処理が行われ、相互認証処理の正常終了後に受け取ったセクタヘッダ領域中の用途識別情報が用途識別回路１１０２に、シードキーが変換テーブル記憶回路１１０３にそれぞれ入力される。用途識別回路１１０２では、内部に再生を許可された用途識別情報に関する情報を有しており、入力された用途識別情報と比較することにより、再生を許可されているか否かを識別し、Ｉ／Ｏ制御回路１１００とメインデータデスクランブル回路１１０５に報告する。一方、シードキーを受領した変換テーブル記憶回路１１０３は、受け取ったシードキーをもとに、シードキーに対応したプリセットデータを乱数発生回路１１０４に出力する。乱数発生回路１１０４は受け取ったプリセットデータをもとに乱数系列を発生してメインデータデスクランブル回路１１０５に出力する。さて、セクタヘッダ領域に引き続いてスクランブルセクタのメインデータが入力される際には、セレクタ１１０１の出力先はメインデータデスクランブル回路１１０５に切り替えられる。その後、メインデータデスクランブル回路１１０５は、セレクタ１１０１から入力されるメインデータと、乱数発生回路１１０４から入力される乱数系列の論理演算を行うことによってデスクランブル処理を実行し、デスクランブル後のデータをオーディオビデオデコーダ回路７０６に出力する。

以上の動作についてのより詳細な説明を図２１を用いて以下に示す。

図２１はデスクランブル回路１１０６において、本発明の第３の実施の形態の情報記録媒体を再生する場合のデスクランブル処理内容を説明するためのフローチャートである。以下にその各処理ステップについて説明する。

（Ｓ１２００）　セレクタ１１０１の出力先を変換テーブル記憶回路１１０３に切り替えて、情報記録媒体のリードイン領域のスクランブル情報セクタから読

み出された変換テーブルを変換テーブル記憶回路１１０３に格納。

（Ｓ１２０１）　セレクタ１１０１の出力先をＩ／Ｏ制御回路１１００に切り替え、スクランブルファイルの再生に先立って受領したセクタヘッダ中のスクランブルフラグをマイクロコントローラ７０２に返送する。マイクロコントローラ７０２はスクランブルフラグが１であるか否かを判定し、Ｉ／Ｏ制御回路１１００に判定結果を返送する。スクランブルフラグが１であると判定されれば（Ｓ１２０２）へ、０であると判定されればメインデータデスクランブル回路１１０５の機能を停止状態として（Ｓ１２０６）へ分岐。

（Ｓ１２０２）　セレクタ１１０１の出力先を用途識別回路１１０２に切り替え、スクランブルファイルの再生に先立って受領したセクタヘッダ中の用途識別情報を転送。用途識別回路１１０２は受け取った用途識別情報と内部に保持している再生許可情報とを比較して、再生が許可されたファイルであるか否かを判定。再生禁止と判定すれば（Ｓ１２０３）へ、再生許可されていると判定すれば（Ｓ１２０４）に分岐。

（Ｓ１２０３）　上記処理ステップ（Ｓ１２０２）で再生禁止のファイルであると判定した場合には、本ステップでＩ／Ｏ制御回路１１００を介してマイクロコントローラ７０２にエラーを報告して処理を終了。

（Ｓ１２０４）　変換テーブル記憶回路１１０３は再生するスクランブルファイルのセクタヘッダから読み出したシードキーを入力され、シードキーと変換テーブルとからプリセットデータを生成し、乱数発生回路１１０４に出力。

（Ｓ１２０５）　セレクタ１１０１の出力先をメインデータデスクランブル回路１１０５に切り替え、メインデータデスクランブル回路１１０５に入力されるスクランブルファイルのメインデータを転送。一方、乱数発生回路１１０４は変換テーブル記憶回路１１０３から入力されたプリセットデータをもとに乱数系列を発生し、メインデータデスクランブル回路１１０５に出力。メインデータデスクランブル回路１１０５では、入力されたメインデータと乱数系列との論理演算を行うことによってデスクランブル処理を実行。

（Ｓ１２０６）　メインデータデスクランブル回路１１０５は、デスクランブ

ル実行時にはデスクランブル後データを、デスクランブル機能を停止状態なら、セレクタ１１０１から入力されたデータをそのままオーディオ／ビデオデコーダ回路７０６に出力。

以上のように、デスクランブル回路１１０６は、用途識別回路を有することにより、再生を禁止された用途識別情報を有するファイルと再生を許可された用途識別情報を有するファイルとを選択的に再生することが可能である。

また、内部にスクランブル識別フラグを分離するセレクタを有するために、スクランブルフラグのみ分離し、デスクランブルを行う／行わないの判定を行うことを可能とする。

また、ディスク単位にプリセットデータに変換するための変換テーブルを決定でき、ファイル単位にシードキーを決定できるため、前記の２つのデータが共にないと再生できないようなセキュリティの高いスクランブル方式をもつ情報記録媒体の再生が可能である。

図２２は、本発明の情報記録媒体の第４の実施の形態を再生するためのデスクランブル回路１３０８の構成を示すブロック図である。以下、各構成要素を説明する。１３００は制御バス７０４との通信を行うためのＩ／Ｏ制御回路を、１３０１は入力されるデータの内容に応じて出力先のブロックを切り替えるセレクタを、１３０２は暗号化ディスク鍵が入力された場合に暗号化ディスク鍵の復号処理を行うディスク鍵復号化回路を、１３０３は暗号化ディスク鍵を復号時に使用するマスター鍵をハードウェア的に格納するマスター鍵格納部を、１３０４はディスク鍵復号回路１３０２で復号されたディスク鍵を受け取り、セクタヘッダ中の暗号化部の復号を行うセクタヘッダ復号回路を、１３０５は媒体識別情報およびセクタヘッダ復号回路１３０４で復号されたオリジナルＣＧＭＳデータと、セレクタから入力されたメディアＣＧＭＳデータの整合性の確認を行うＣＧＭＳ検査回路を、１３０６はセクタヘッダ復号回路１３０４で復号された用途識別情報を受け取って再生が許可されているか否かを判定する用途識別回路を、１３０７はセクタヘッダ復号回路１３０４から入力されるタイトル鍵をもとにセレクタ１３０１から入力されるメインデータをデスクランブルするメインデータデスクランブル回路を、それぞれが示している。

以下に、デスクランブル回路１３０８の動作を説明する。

まず、相互認証処理が正常に終了した後にリードイン領域に記録されたスクランブル情報セクタを読み出す場合、Ｉ／Ｏ制御回路１３００を介してセレクタ１３０１の出力先がディスク鍵復号回路１３０２に設定され、入力された読み出しデータはセレクタ１３０１を介してディスク鍵復号化回路１３０２に入力される。ディスク鍵復号化回路１３０２では、マスター鍵格納部１３０３から入力されるマスター鍵をもとにディスク鍵を復号し、ディスク鍵復号化回路１３０２の内部に格納される。

一方、スクランブルファイルの再生時には、データの再生に先立って相互認証処理が行われ、相互認証処理の正常に終了すれば、再生するスクランブルファイルのセクタヘッダがセレクタ１３０１に入力される。セレクタ１３０１はセクタヘッダの内容毎に出力先を選定し、スクランブルフラグをＩ／Ｏ制御回路１３００を介してマイクロコントローラ７０２に、メディアＣＧＭＳデータをＣＧＭＳ検査回路１３０６に、暗号化オリジナルＣＧＭＳデータおよび暗号化用途識別情報および暗号化タイトル鍵（以下では、これらをあわせて暗号化セクタヘッダと称す）をセクタヘッダ復号回路１３０４に出力する。セクタヘッダ復号回路１３０４はディスク鍵復号回路１３０２からディスク鍵を受領し、ディスク鍵をもとに暗号化セクタヘッダを復号し、オリジナルＣＧＭＳデータをＣＧＭＳ検査回路１３０５に、用途識別情報を用途識別回路１３０６に、タイトル鍵をメインデータデスクランブル回路１３０７に、それぞれ出力する。ＣＧＭＳ検査回路１３０５はセレクタ１３０１から入力されるメディアＣＧＭＳデータとセクタヘッダ復号回路１３０４から入力されるオリジナルＣＧＭＳとを受け取り、再生の許可された値か否かを判定する。この時、ＣＧＭＳ検査回路１３０５の判定の基準を（表２）に示す。（ただし、メディアＣＧＭＳデータとオリジナルＣＧＭＳデータが示す意味については、本発明の第４の実施の形態の情報記録媒体の説明に準ずるものとする。）

表2

媒体識別情報	メディアCGMS データ	オリジナルCGMS データ	CGMS 判定情報
1 (再生専用型媒体)	00	00	1
		01/10/11	0
	01	00/01/10/11	0
	10	00/01/11	0
		10	1
	11	00/01/10	0
		11	1
0 (書換型媒体)	00	00	1
		01/10/11	0
	01/10	00/01/10/11	0
	11	10	1
		00/01/11	0

（表2）において、CGMS判定情報が1を示す場合には、再生可能であるとしてメインデータデスクランブル回路１３０７とマイクロコントローラ７０２に報告する。一方、CGMS判定情報が0の場合には不正コピー等の行われた可能性があることを意味する妥当でない値であるとして、メインデータデスクランブル回路１３０７およびマイクロコントローラ７０２にエラーを報告する。例えば、（表2）において、媒体識別情報が書換型媒体を示す0であって、メディアCGMSデータがコピー禁止を示す11であって、オリジナルCGMSデータが1回コピーのみ許可を示す10である場合には、1回のみコピー許可のファイルが書換型媒体に既に1回コピーをされてメディアCGMSデータのみが11となってコピー禁止に変更されたと考えられるため、出力は再生許可を意味する1となっている。一方、仮に上記のような1回のみコピー許可であるファイルが不正なコピーをされた場合には、メディアCGMSデータとオリジナルCGMSデータが共に1回のみコピー許可を意味する10となるために、その場合のCGMS判定情報は再生禁止を意味する0となっている。一方、用途識別回路１３０６は、再生の許可されている用途識別情報を内部に有しており、その情報とセクタヘッダ復号回路１３０４から入力される用途識別情報を比較して、スクランブルファイルが再生を許可された用途であるか否かを判定する。再生の許可されていない

用途識別情報であった場合には、マイクロコントローラ７０２およびメインデータデスクランブル回路１３０７にエラーを報告する。スクランブルファイルのデータを再生する場合には、セレクタ１３０１の出力先はメインデータデスクランブル回路１３０７に切り替えられ、入力される読み出しデータはメインデータデスクランブル回路１３０７に転送される。メインデータデスクランブル回路１３０７は、セクタヘッダ復号回路１３０４からタイトル鍵を受け取り、受け取ったタイトル鍵をもとにスクランブルデータのデスクランブル処理を施してオーディオ／ビデオデコーダ回路７０６に出力する。

以上のように、デスクランブル回路１３０８は暗号化ディスク鍵、暗号化タイトル鍵の復号を行い、タイトル鍵が再生の許可されたものであれば、メインデータのデスクランブル処理を行って、スクランブル後のディジタルＡＶデータをオーディオ／ビデオデコーダ回路７０６に出力する。

次に、デスクランブル回路１３０８におけるスクランブルファイルの再生処理の動作について、図２３のフローチャートを用いて説明する。以下に各ステップの処理内容を示す。

（Ｓ１４００）　読み出しデータにリードイン領域の暗号化ディスク鍵情報が入力される場合に、セレクタ１３０１の出力先はディスク鍵復号回路１３０２に設定され、暗号化ディスク鍵をディスク鍵復号回路１３０２に転送。ディスク鍵復号回路１３０２はマスター鍵格納部１３０３からマスター鍵を受け取り暗号化ディスク鍵を復号し、復号されたディスク鍵をセクタヘッダ復号回路１３０４に出力。

（Ｓ１４０１）　再生に先立って読み出されたスクランブルファイルのセクタヘッダから、セレクタ１３０１はスクランブルフラグを分離し、Ｉ／Ｏ制御回路１３００を介してマイクロコントローラ７０２に転送。マイクロコントローラ７０２はスクランブルフラグが１であるか否かを判定。判定結果が、１であれば（Ｓ１４０２）へ、１でなければ（Ｓ１４０７）へ分岐。

（Ｓ１４０２）　再生に先立って読み出されたスクランブルファイルのセクタヘッダから、セレクタ１３０１は暗号化セクタヘッダを分離し、セクタヘッダ復

号回路１３０４へ転送。セクタヘッダ復号回路１３０４は、あらかじめディスク鍵復号回路１３０２から受け取ったディスク鍵をもとに、受け取った暗号化セクタヘッダを復号し、内容毎に分離し、オリジナルＣＧＭＳデータをＣＧＭＳ検査回路１３０５に、用途別識別情報を用途識別回路１３０６に、タイトル鍵をメインデータデスクランブル回路１３０７に、それぞれ出力。

（Ｓ１４０３）　ＣＧＭＳ検査回路１３０５は、マイクロコントローラ７０２から受け取った媒体識別情報と、セレクタ１３０１から受け取ったメディアＣＧＭＳデータと、セクタヘッダ復号回路１３０４から受け取ったオリジナルＣＧＭＳデータから、（表２）に応じたＣＧＭＳ判定情報を出力。ただし、（表２）において、ＣＧＭＳ判定情報が１の場合には、Ｉ／Ｏ制御回路１３００とメインデータデスクランブル回路１３０７に正常なＣＧＭＳ制御情報であることを報告。

（Ｓ１４０４）　ＣＧＭＳ判定結果が０であった場合にはＣＧＭＳ検査回路１３０５が、用途識別情報が再生を禁止された用途であった場合には用途識別回路１３０６が、Ｉ／Ｏ制御回路１３００およびメインデータデスクランブル回路１３０７にエラーを報告し、再生処理を終了する。

（Ｓ１４０５）　用途識別回路１３０６は、セクタヘッダ復号回路１３０４から受け取った用途識別情報を判定し、再生を許可された場合にはＩ／Ｏ制御回路１３００およびメインデータデスクランブル回路１３０７に再生を許可されたファイルであることを報告。

（Ｓ１４０６）　セレクタ１３０１は、読み出しデータとしてスクランブルファイルのメインデータを受け取ると、出力先をメインデータデスクランブル回路１３０７に設定し、メインデータを転送。メインデータデスクランブル回路１３０７はセクタヘッダ復号回路１３０４から受け取ったタイトル鍵をもとに、入力されたメインデータのデスクランブル処理を実行。

（Ｓ１４０７）　メインデータデスクランブル回路１３０７は、デスクランブル処理を実行した場合にはデスクランブル後のメインデータを、デスクランブル処理を実行しなかった場合にはセレクタ１３０１から入力されたデータをそのままオーディオ／ビデオデコーダ回路７０６に出力。

以上のように、デスクランブル回路１３０８は、用途識別回路を有することにより、再生を禁止された用途識別情報を有するファイルと再生を許可されたようと識別情報を有するファイルとを選択的に再生することが可能である。

また、内部にスクランブル識別フラグを分離するセレクタを有するために、スクランブルフラグのみ分離し、デスクランブルを行う／行わないの判定を行うことを可能とする。

また、本発明の情報記録媒体の第４の実施の形態のような階層的に暗号／スクランブル化されたセキュリティの高いディスクであっても、ディスク鍵復号回路、セクタヘッダ復号回路、メインデータデスクランブル回路が連携して動作することにより、デスクランブルを行わないときと同様に処理することが可能となる。

また、ＣＧＭＳ検査回路１３０５を有することによって、不正にコピーされたデータを検出することが可能となり、不正コピーデータの再生を防止することが可能となる。さらに、コピーが何度繰り返されたデータであるかという、コピーの世代を管理することが可能となり、ある定められた回数のみのコピー動作を許可するようなソフトウェアが記録された情報記録媒体の著作権を保護する機構を有する。

図２４は、光ディスクドライブ５０９内のデコーダ認証回路６０１の詳細な構成を示すブロック図である。以下、各構成要素について説明する。１５００はマイクロコントローラ６０２との通信を行うための入出力制御を行うＩ／Ｏ制御回路を、１５０１はＩ／Ｏ制御回路１５００から入力される時変鍵をもとに乱数を発生する乱数発生回路を、１５０２は関数を決定するための第１の入力（図２４ではｋと表記）よって関数fkを決定し、その引数となる第２の入力（図２４ではＲ１と表記）から関数値fk(R1)を計算して出力する関数fk(R1)生成回路を、同様に１５０３はｋとＲ２から関数gk(R2)を計算して出力すると共にＩ／Ｏ制御回路１５００から入力されるデコーダ応答データとの比較を行う関数gk(R2)生成・比較回路を、１５０４は関数gk(R2)生成・比較回路１５０３と関数fk(R1)生成回路１５０２から出力される２つの関数値をもとにバス鍵を生成するバス鍵生成回路

を、１５０５はバス鍵生成回路１５０４から出力されるバス鍵に従ってデータ再生回路６０６から出力されるデータを暗号化するバス暗号化回路を、それぞれ示している。

以下、デコーダ認証回路６０１の動作を説明する。

光ディスクドライブ５０９のリセット時やディスク交換時に、マイクロコントローラ６０２はディスクのリードイン領域のスクランブル情報セクタのセクタヘッダ領域から読み出した相互認証鍵ｋをＩ／Ｏ制御回路１５００を介して関数ｆｋ(R1)生成回路１５０２および関数ｇｋ(R2)生成・比較回路１５０３にあらかじめ設定する。

関数ｆｋ(R1)生成回路１５０２は相互認証鍵ｋを内部的に保持しており、その後の相互認証処理時に乱数値Ｒ１が入力された場合に関数値ｆｋ(R1)を計算し、バス鍵生成回路１５０４およびＩ／Ｏ制御回路１５００に出力する。

バス鍵生成回路１５０４は入力された関数値ｆｋ(R1)を内部的に格納する。引き続き、マイクロコントローラ６０２からＩ／Ｏ制御回路１５００を介して乱数発生のための時変鍵が入力された場合に乱数発生回路１５０１は、時変鍵をもとに乱数Ｒ２を発生してＩ／Ｏ制御回路１５００に返送すると共に、関数ｇｋ(R2)生成・比較回路１５０３に出力する。

乱数Ｒ２を受け取った関数ｇｋ(R2)生成・比較回路１５０３は、前もって保持していた相互認証鍵ｋおよび乱数値Ｒ２から関数値ｇｋ(R2)を計算して内部的に保持する。更に関数ｇｋ(R2)生成・比較回路１５０３は、Ｉ／Ｏ制御回路１５００からデコーダ応答データを受け取り、内部で計算した関数値ｇｋ(R2)と比較を行う。比較の結果、ｇｋ(R2)の値とデコーダ応答データが一致しなかった場合には、Ｉ／Ｏ制御回路１５００を介してマイクロコントローラ６０２に相互認証処理でエラーが発生したことを報告する。相互認証処理に失敗した場合には、相互認証処理に続く暗号化ディスク鍵および暗号化タイトル鍵の転送等の処理は中止される。

一方、ｇｋ(R2)とデコーダ応答データの２つの値が一致した場合は相互認証処理が正常に終了したと判定され、関数値ｆｋ(R2)がバス鍵生成回路１５０４に出力される。この時、バス鍵生成回路１５０４は、関数値ｆｋ(R1)およびｇｋ(R2)が正常に

入力された場合にのみ、２つの関数値ｆｋ(R1)およびｇｋ(R2)をもとにバス鍵を生成し、バス暗号化回路１５０５に出力する。

バス暗号化回路１５０５は、Ｉ／Ｏ制御回路１５００を介してマイクロコントローラ６０２からモードを切り替えるための制御信号（以下、モード制御信号と称す）を受け取り、モードがディスク鍵再生モードであるか、またはタイトル鍵再生モードであれば、データ再生回路６０６から入力される暗号化ディスク鍵又は暗号化タイトル鍵に対して、あらかじめ入力されたバス鍵をもとに所定の暗号化を施し、ＳＣＳＩ制御回路６００に出力する。

一方、暗号化タイトル鍵の送出後に、実際のファイルデータを送出する場合には、モード制御信号はデータ再生モードに切り替えられ、バス暗号化回路１５０５はバス暗号化は行わずにデータ再生回路６０６から出力されるデータをそのままＳＣＳＩ制御回路６００に出力する。

以上のようにデコーダ認証回路６０１では、相互認証処理において相互認証鍵で決定される関数値計算を行って、デコーダから送られる関数値と一致した場合のみ相互認証処理を正常に終了する。更に、再生動作においても、暗号化ディスク鍵、暗号化タイトル鍵の転送時には、相互認証処理において生成したバス鍵を用いて更に暗号化した鍵情報を送出する処理を行う。

次に、ＡＶデコーダカード５０７およびＳＣＳＩ制御回路内蔵ＡＶデコーダカード８０１上のドライブ認証回路７０１の構成および動作について図面を参照して説明する。

図２５は、ドライブ認証回路７０１の構成を示すブロック図である。以下、各構成要素について説明する。１６００はマイクロコントローラ７０２との制御信号の送受信を行うためのＩ／Ｏ制御回路を、１６０１はＩ／Ｏ制御回路１６００から時変鍵を受信して乱数Ｒ１を発生し、Ｉ／Ｏ制御回路１６００に返送すると共に関数ｆｋ(R1)生成・比較回路１６０３に出力する乱数発生回路を、１６０２は関数ｆｋ(R1)生成・比較回路１６０３から入力される定数ｋとＩ／Ｏ制御回路１６００から入力される乱数Ｒ２をもとに関数ｇｋ(R2)を計算する関数ｇｋ(R2)生成回路を、１６０３は乱数発生回路１６０１から入力される乱数Ｒ１をもとにｋが１か

らnまでについて関数fk(R1)の値を計算して、Ｉ／Ｏ制御回路１６００から入力されるドライブ応答データと一致するか比較する関数fk(R1)生成・比較回路を、１６０４は関数gk(R2)生成回路１６０２から出力される関数値と関数fk(R1)生成・比較回路１６０３から出力される関数値からバス鍵を生成するバス鍵生成回路を、１６０５はバス鍵生成回路１６０４から出力されるバス鍵によってデータの復号を行うバス復号化回路を、それぞれいう。

次に、ドライブ認証回路７０１の動作を説明する。

まず、相互認証処理の開始時にドライブ認証回路７０１は、Ｉ／Ｏ制御回路１６００を介してマイクロコントローラ７０２から乱数発生のための時変鍵を受け取り、乱数発生回路１６０１によって乱数が発生される。

乱数発生回路１６０１は発生した乱数Ｒ１を関数fk(R1)生成・比較回路１６０３およびマイクロコントローラ７０２に出力する。その後、関数fk(R1)生成・比較回路１６０３は、マイクロコントローラ７０２からドライブ応答データを受け取り、内部に保持している乱数値Ｒ１を引数として関数f1(R1),f2(R1),f3(R1)・・・を計算し、ドライブ応答データとfk(R1)が一致する様なkを求める。この時、保持している全ての関数計算を行ってもドライブ応答データと一致するkを求めることができなかった場合に関数fk(R1)生成・比較回路１６０３は、認証結果としてエラーをＩ／Ｏ制御回路１６００を介してマイクロコントローラ７０２に返送する。

一方、ドライブ応答データとfk(R1)が一致するようなkが発見された場合は、認証結果として正常終了をマイクロコントローラ７０２に返送し、kを関数gk(R2)生成回路１６０２に出力し、関数値fk(R1)をバス鍵生成回路１６０４に出力する。正常にkの値を発見できた場合にドライブ認証回路７０１は、引き続いて乱数Ｒ２をマイクロコントローラ７０２から受け取り関数gk(R2)生成回路１６０２に入力する。関数gk(R2)生成回路１６０２は、あらかじめ関数fk(R1)生成・比較回路１６０３から受け取った値kと、入力された乱数Ｒ２から関数gk(R1)を計算し、計算した関数値をマイクロコントローラ７０２およびバス鍵生成回路１６０４に出力する。

バス鍵生成回路１６０４は前もって受け取った関数値fk(R1)と、gk(R2)の２つの関数値をもとにバス鍵を生成し、バス復号回路１６０５に出力する。一方、マイクロコントローラ７０２に送出した関数値gk(R2)が光ディスクドライブ５０９で正常に認証された場合には、マイクロコントローラ７０２がモード制御信号を切り替えて、バス復号化回路１６０５のモードをディスク鍵再生モードまたはタイトル鍵再生モードに切り替え、復号処理機能使用状態とする。

この時、ＳＣＳＩ制御回路９００又はシステムインタフェース回路７００から入力されるデータ（暗号化ディスク鍵又は暗号化タイトル鍵）はバス復号化回路１６０５においてあらかじめ保持されているバス鍵によって復号される。ただし、バス復号化回路１６０５によって復号されるのはバス鍵によるバス暗号のみであり、マスター鍵によって暗号化された暗号化ディスク鍵、ディスク鍵によって暗号化された暗号化タイトル鍵は暗号化されたままデスクランブル回路７０５に出力される。

またその後に、スクランブルファイルの再生データがＳＣＳＩ制御回路９００又はシステムインタフェース回路７００から入力される際にバス復号化回路１６０５は、マイクロコントローラ７０２からのモード制御信号によってデータ再生モードに切り替えられ、バス鍵による復号処理を行わずにデスクランブル回路７０５にデータをそのまま転送する。

以上のようにドライブ認証回路７０１では、内部で発生した乱数から複数の関数値を計算し、そのうちのいずれか一つとドライブ応答データが一致することでドライブを認証し、逆に乱数を受領して内部の関数値を計算して返送することで光ディスクドライブ５０９から認証されるという、相互認証処理を実行する。

また、再生動作においても、暗号化ディスク鍵、暗号化タイトル鍵の受信時には、相互認証処理において生成したバス鍵を用いて復号処理を行う。

次に、本発明の情報再生装置の第５の実施の形態および第６の実施の形態において実行される相互認証処理のプロトコルについて図面を参照して説明する。

図２６は、光ディスクドライブ５０９とＡＶデコーダカード５０７又はＳＣＳＩ制御回路内蔵ＡＶデコーダカード８０１間の相互認証処理を説明するためのフ

ローチャートである。

相互認証処理は、装置のリセット時やディスク交換時、および読み出そうとしたファイルがスクランブルファイルであることがファイル管理情報から確認された時等に、適宜実行される。以下、各処理ステップについて説明する。ただし、ＡＶデコーダカード５０７またはＳＣＳＩ制御回路内蔵ＡＶデコーダカード８０１を、以下では単にＡＶデコーダと称することとする。また、以下では、ＳＣＳＩプロトコル上でのコマンドを、デバイスコマンドと称する。

（Ｓ１７００）ＡＶデコーダは、タイマー等を用いて発生させた時間と共に変化する時変鍵をもとに乱数Ｒ１を生成。

（Ｓ１７０１）光ディスクドライブはデバイスコマンド"Send R1"によって、ＡＶデコーダが生成した乱数Ｒ１を受け取る。この時光ディスクドライブは、装着されているディスクの相互認証鍵ｋを未だ格納していなければ、リードイン領域のスクランブル情報セクタのセクタヘッダ領域から相互認証鍵の読み出しを実行。

（Ｓ１７０２）光ディスクドライブがステップ（Ｓ１７０１）の処理中に何らかのエラーを検出してエラー報告が行われた場合には、ステップ（Ｓ１７１３）に分岐、正常に終了すればステップ（Ｓ１７０３）に分岐。

（Ｓ１７０３）光ディスクドライブは、デバイスコマンド"Report fk(R1)"を受領し、あらかじめ受け取った乱数値Ｒ１とディスクから読み出した相互認証鍵ｋの値をもとに、関数fk(R1)の値を計算し、計算結果をＡＶデコーダに返送する。以上の処理において何らかのエラーが生じた場合に光ディスクドライブは、コマンドの処理結果としてエラーを報告。

（Ｓ１７０４）デバイスコマンド"Report fk(R1)"処理中に何らかのエラーが発生し、コマンド処理結果がエラーとなっていればステップ（Ｓ１７１３）に分岐、処理結果が正常終了であればステップ（Ｓ１７０５）に分岐。

（Ｓ１７０５）ＡＶデコーダは、内部に保持する関数値生成回路を使用して、１からｎ（ｎは正の整数）までのｉ（ｉは正の整数）について関数値fi(R1)を計算し、計算したfi(R1)の値と、（Ｓ１７０３）において光ディスクドライブから

返送されたfk(R1)の値を比較する。ＡＶデコーダはfi(R1)=fk(R1)となるようなｉの値を検出すれば、その値を内部的に保持。

（Ｓ１７０６）前記処理ステップ（Ｓ１７０５）において、ＡＶデコーダがfi(R1)=fk(R1)となるようなｉを検出できなかった場合にはステップ（Ｓ１７１３）に分岐、検出した場合にはステップ（Ｓ１７０７）に分岐。

（Ｓ１７０７）光ディスクドライブはデバイスコマンド"Report R2"コマンドを受け取り、内部の乱数発生機構で時間と共に変化する時変鍵をもとに乱数を発生し、ＡＶデコーダに転送する。なお、本ステップで光ディスクドライブが何らかのエラーを検出した場合には、エラーを報告。

（Ｓ１７０８）前記ステップ（Ｓ１７０７）において、"Report R2"コマンド実行過程で、何らかのエラーが発生した場合にはステップ（Ｓ１７１３）に分岐、正常に終了した場合にはステップ（Ｓ１７０９）に分岐。

（Ｓ１７０９）（Ｓ１７０８）において"Report R2"コマンドによって光ディスクドライブが発生した乱数Ｒ２を受け取ったＡＶデコーダは、内部の関数計算回路を使用して、既にステップ（Ｓ１７０５）において格納した定数ｋ（＝ｉ）と、ステップ（Ｓ１７０７）において光ディスクドライブから受信した乱数値Ｒ２をもとに、関数値gk(R2)を計算。

（Ｓ１７１０）関数値gk(R2)を計算したＡＶデコーダは、デバイスコマンド"Snd gk(R2)"を実行して、ステップ（Ｓ１７０９）において計算した関数値を光ディスクドライブに転送する。関数値gk(R2)を受け取った光ディスクドライブは、

内部に有する関数計算回路において、相互認証鍵ｋと乱数値Ｒ２を用いてgk(R2)を計算する。その後光ディスクドライブは、ＡＶデコーダから受け取った関数値gk(R2)と、内部の計算回路によって計算したgk(R2)とを比較し、一致した場合には正常終了を処理結果として報告する。一方、コマンド処理中に何らかのエラーが生じた場合や、受信した関数値と内部で計算した関数値とが一致しなかった場合には、コマンド処理結果としてエラーを報告。

（Ｓ１７１１）前記ステップ（Ｓ１７１０）において、コマンド処理結果がエ

ラーであればステップ（Ｓ１７１３）に分岐、正常終了であれば（Ｓ１７１２）に分岐。

（Ｓ１７１２）ＡＶデコーダは、上記の相互認証処理中において取得した２つの関数値f(R1)およびf(R2)をもとに、内部に保持するバス鍵生成回路を用いてバス鍵ＢＫを生成する。同様に、光ディスクドライブも、上記相互認証処理中に取得した２つの関数値から内部に保持するバス鍵生成回路を用いてバス鍵ＢＫを生成。（ここで、光ディスクドライブとＡＶデコーダが相互認証処理中で、生成されるバス鍵ＢＫは同一となる）。

（Ｓ１７１３）デバイスコマンド実行中にエラーが生じた場合、本ステップにおいてエラー報告と共に相互認証処理を中止。

以上のように相互認証処理を行うことによって、不正コピーを行う機器へのデータ転送でないことを光ディスクドライブが確認した後に鍵情報を転送することができるために、デスクランブルを行うための鍵情報を隠す効果がある。従って、スクランブル方式の不正な解読を防止する効果がある。

また、ＡＶデコーダがデータを受け取る機器が不正コピーしたデータを転送する機器でないことを確認した後に鍵情報の復号化およびデータのデスクランブルを行うことができるために、不正コピーされたデータ再生を防止する効果がある。

また、相互認証処理の度に異なるバス鍵を生成するために、鍵情報を不正に読み出されることを防止すると共に、暗号化／スクランブル方式の不正な解読を防止する効果がある。

また、相互認証において光ディスクドライブがＡＶデコーダを認証する場合と、ＡＶデコーダが光ディスクドライブを認証する場合とで、異なる関数を用いているために、相互認証動作を不正に実行することを目的として相互認証動作の方式を解読しようとする行為に対するセキュリティが高い。

また、相互認証処理において、光ディスクドライブ、ＡＶデコーダの各々が生成した時変鍵を用いているために、相互認証処理を実行する度に異なる乱数値が発生され、異なる関数値が転送され、異なるバス鍵が生成されるため、相互認証

動作を不正に実行することを目的として相互認証動作の方式を解読しようとする行為に対するセキュリティが高い。

また、情報記録媒体上に記録された相互認証鍵を相互認証処理に用いることにより、相互認証動作を不正に実行することを目的として相互認証動作の方式を解読しようとする行為に対するセキュリティが高い。

なお、上記説明では、情報記録媒体として本発明の情報記録媒体の第４の実施の形態を例に説明したが、本発明の情報記録媒体の第３の実施の形態についても同様に処理することが可能である。

産業上の利用の可能性

本発明の情報記録媒体は、リードイン領域とデータ記録領域とを有している。リードイン領域に記録された鍵情報に基づいて、データ記録領域に記録されたスクランブルされたデータがデスクランブルされる。このように、リードイン領域に鍵情報を記録することにより、セキュリティが向上する。情報記録媒体のドライブ装置は、リードイン領域を直接的にアクセスすることができるのに対し、ドライブ装置以外の装置（例えば、パーソナルコンピュータ）は、リードイン領域を直接的にアクセスすることができないからである。さらに、リードイン領域に鍵情報を記録することにより、鍵情報を読み出すための専用の読み出し手段を設ける必要がない。

本発明の他の情報記録媒体は、リードイン領域とデータ記録領域とを有している。リードイン領域に記録された第１の鍵情報とデータ記録領域に記録された第２の鍵情報とに基づいて、スクランブルされたデータがデスクランブルされる。このように、デスクランブルのための鍵情報が二重化されているため、セキュリティが向上する。

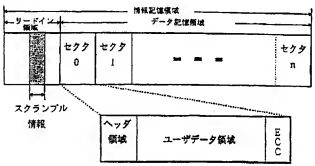
本発明の情報再生装置によれば、スクランブルされたデータがデコード装置に送信される前に、相互認証処理が行われる。相互認証処理により相手方が正規であることが相互に確認される。これにより、セキュリティが向上する。

本発明の情報再生装置によれば、読み出し装置とデコード装置との間で相互認証処理が行われる。相互認証処理が正常に終了すると、読み出し装置とデコード

装置とに共通なバス鍵情報が生成され、バス鍵情報によって暗号化された鍵情報が読み出し装置からデコード装置に送信される。このように、相互認証処理を行った後、さらに共通のバス鍵を使用することにより、相手方が正規であることが相互に確認される。これにより、セキュリティが向上する。

【図1】

図1



【図2】

図2

スクランブル情報	選択する初期値テーブル
0 0	テーブル0
0 1	テーブル1
1 0	テーブル2
1 1	テーブル3

(a)

テーブル0

ビット列	初期値
0 0 0	0000 h
0 0 1	0100 h
・・・	・・・
1 1 1	0700 h

テーブル1

ビット列	初期値
0 0 0	0000 h
0 0 1	0010 h
・・・	・・・
1 1 1	0070 h

テーブル2

ビット列	初期値
0 0 0	0000 h
0 0 1	0001 h
・・・	・・・
1 1 1	0007 h

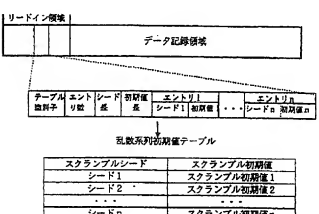
テーブル3

ビット列	初期値
0 0 0	000F h
0 0 1	00F0 h
・・・	・・・
1 1 1	0FFF h

(b)

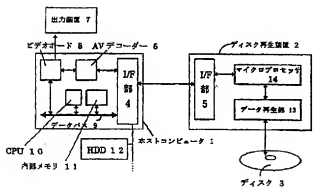
【図3】

図3



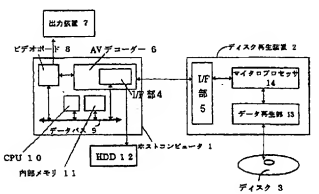
【図4】

図4



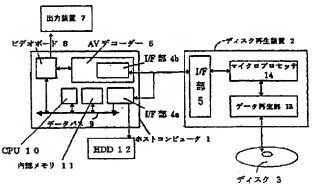
【図5】

図5



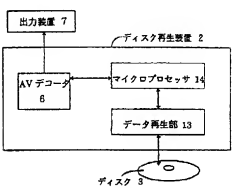
【図6】

図6



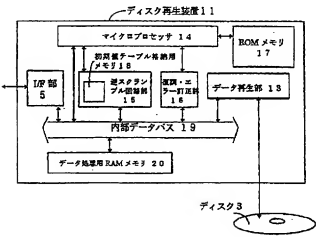
【図7】

図7



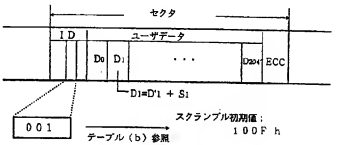
【図８】

図８



【図９】

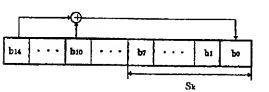
図９



（a）

ビット列	スクランブル初期値	乱数系列			
		S0	S1	・・・	S2047
０００	0000h	A0	A1	・・・	A2047
００１	100F h	B0	B1	・・・	B2047
・・・	・・・			・・・	
１１１	5FFF h	C0	C1	・・・	C2047

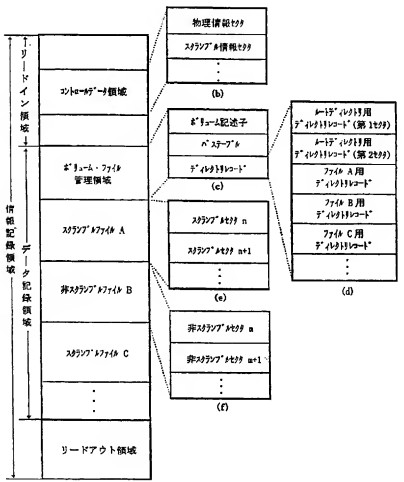
（b）



（c）

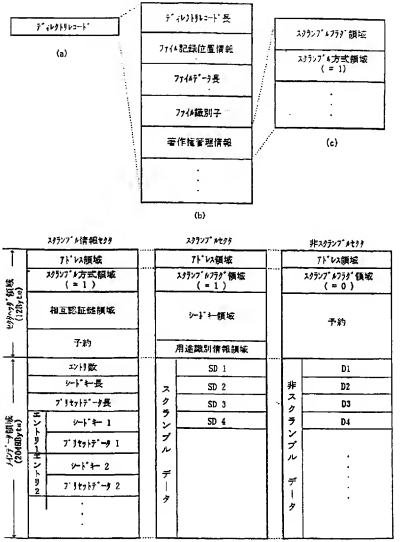
【図１０】

図１０



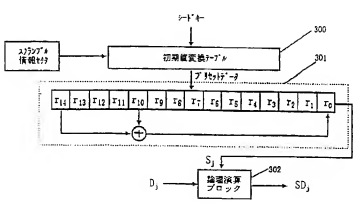
【図１１】

図１１



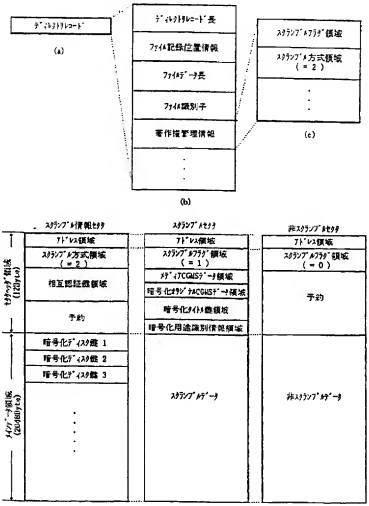
【図１２】

図１２



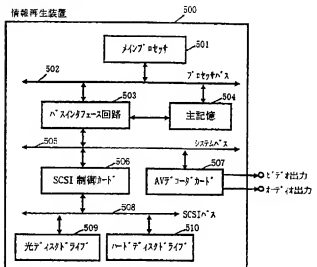
【図１３】

図１３



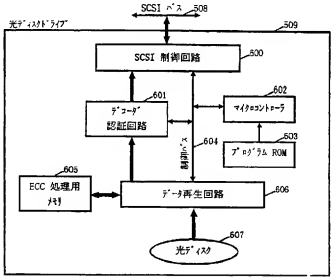
【図１４】

図１４



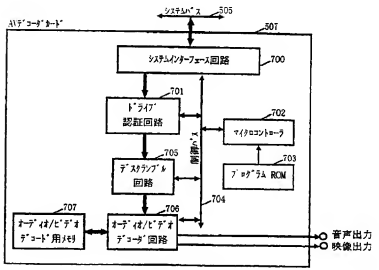
【図１５】

図１５



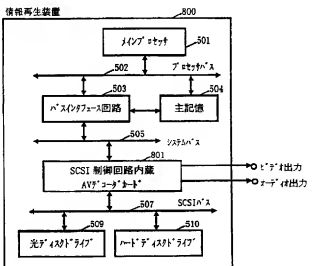
【図16】

図16



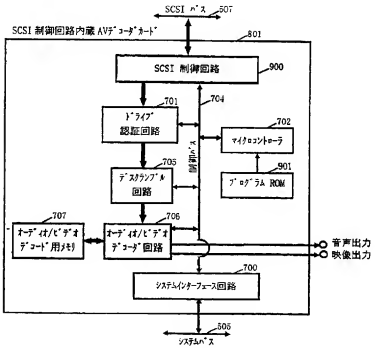
【図17】

図17



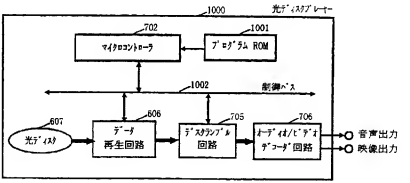
【図18】

図18



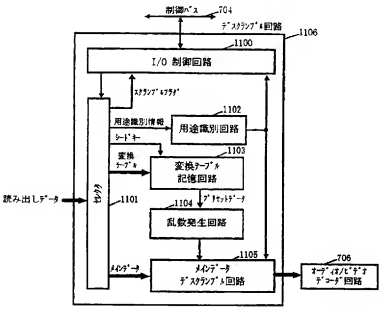
【図19】

図19



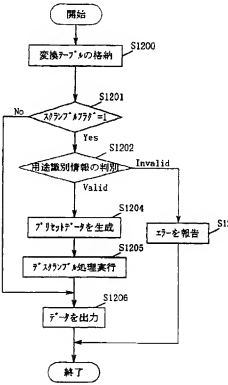
【図２０】

図２０



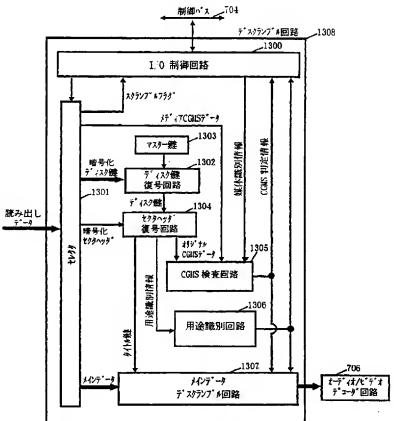
【図２１】

図２１



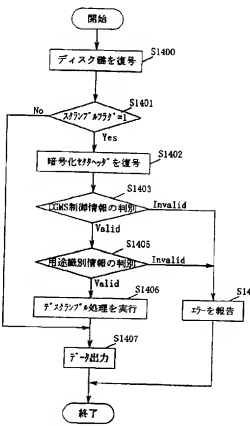
【図２２】

図２２



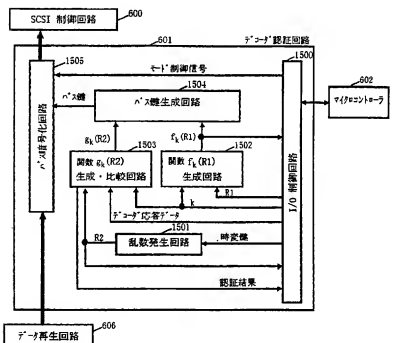
【図２３】

図２３



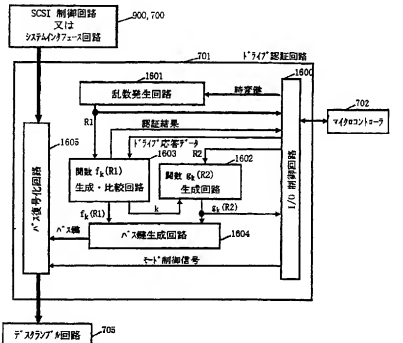
【図２４】

図２４



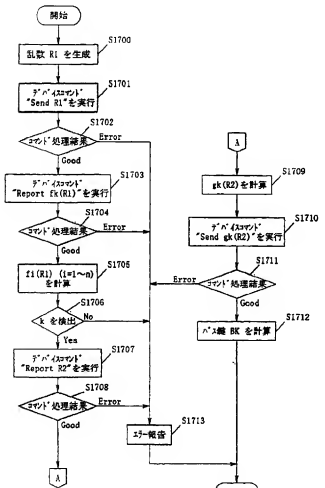
【図２５】

図２５



【図２６】

図２６



【国際調査報告】

国際調査報告　　国際出願番号　PCT/JP96/02901

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl⁶ G11B19/00

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl⁶ G11B19/00, G11B20/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国　実用新案公報　1926－1996
日本国　公開実用新案公報　1971－1996
日本国　登録実用新案公報　1994－1996

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP, 62－89275, A (三洋電機株式会社) 23. 4月. 1987 (23. 04. 87) (ファミリーなし)	1
A	JP, 7－85574, A (日本ビクター株式会社) 31. 3月 1995 (31. 03. 95) (ファミリーなし)	1－26
A	JP, 7－21688, A (日本ビクター株式会社) 24. 1月. 1995 (24. 01. 95) (ファミリーなし)	1－26
A	JP, 7－249264, A (株式会社インテック, ブラザー工業株式会社) 26. 9月. 1995 (26. 09. 95) (ファミリーなし)	1－26

☒ Cの欄にも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」先行文献ではあるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
28. 01. 97	12.02.97

名称及びあて先	特許庁審査官（権限のある職員）	5D 7618
日本国特許庁（ISA/JP） 郵便番号100 東京都千代田区霞が関三丁目4番3号	菅藤 邦二　印	
	電話番号　03－3581－1101　内線　6921	

様式PCT/ISA/210（第2ページ）（1992年7月）

国際調査報告 国際出願番号 PCT/JP96/02901

C（続き）．引用文献のカテゴリー*	関連すると認められる文献 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP, 4-256196, A (株式会社東芝) 10. 9月. 1992 (10. 09. 92) (ファミリーなし)	2-4
A	JP, 6-133314, A (松下電器産業株式会社) 13. 5月. 1994 (13. 05. 94) (ファミリーなし)	1-26
A	JP, 6-163307, A (ソニー株式会社) 14. 6月. 1994 (14. 06. 94) (ファミリーなし)	1-26
P	JP, 7-288798, A (三菱電機株式会社) 31. 10月. 1995 (31. 10. 95) (ファミリーなし)	1-26

様式PCT/ISA/210（第2ページの続き）（1992年7月）

フロントページの続き

(72)発明者 松崎 なつめ
大阪府箕面市粟生間谷西11H6-7-803